460ETCMRS - Protocol Gateway

Product User Guide

Software Build Date: January 15th, 2015
Version 3

Trademarks

CompactLogix, ControlLogix, & PLC-5 are registered trademarks of Rockwell Automation, Inc. EtherNet/IP is a trademark of the ODVA. MicroLogix, RSLogix 500, and SLC are trademarks of Rockwell Automation, Inc. Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation. BACnet® is a registered trademark of American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). All other trademarks and registered trademarks are the property of their holders.

Limited Warranty

Real Time Automation, Inc. warrants that this product is free from defects and functions properly.

EXCEPT AS SPECIFICALLY SET FORTH ABOVE, REAL TIME AUTOMATION, INC. DISCLAIMS ALL OTHER WARRANTIES, BOTH EXPRESSED AND IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR APPLICATION. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular application, Real Time Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams. Except as specifically set forth above, Real Time Automation and its distributors and dealers will in no event be liable for any damages whatsoever, either direct or indirect, including but not limited to loss of business profits, income, or use of data. Some states do not allow exclusion or limitation of incidental or consequential damages; therefore, the limitations set forth in this agreement may not apply to you.

No patent liability is assumed by Real Time Automation with respect to use of information, circuits, equipment, or software described in this manual.

Government End-Users

If this software is acquired by or on behalf of a unit or agency of the United States Government, this provision applies: The software (a) was developed at private expense, is existing computer software, and was not developed with government funds; (b) is a trade secret of Real Time Automation, Inc. for all purposes of the Freedom of Information Act; (c) is “restricted computer software” submitted with restricted rights in accordance with subparagraphs (a) through (d) of the Commercial “Computer Software-Restricted Rights” clause at 52.227-19 and its successors; (d) in all respects is proprietary data belonging solely to Real Time Automation, Inc.; (e) is unpublished and all rights are reserved under copyright laws of the United States. For units of the Department of Defense (DoD), this software is licensed only with “Restricted Rights”: as that term is defined in the DoD Supplement of the Federal Acquisition Regulation 52.227-7013 (c) (1) (ii), rights in Technical Data and Computer Software and its successors, and: Use, duplication, or disclosures is subject to restrictions as set forth in subdivision (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 52.227-7013. If this software was acquired under GSA schedule, the U.S. Government has agreed to refrain from changing or removing any insignia or lettering from the Software or documentation that is provided or from producing copies of the manual or media. Real Time Automation, Inc.

© 2015 Real Time Automation, Inc. All rights reserved.

Overview 5
Required Tools and Data 6
Powering The Gateway 7
Accessing the Main Page 8
Error: Main Page Does Not Launch 9
Main Page 10
Device Configuration 11
Port Configuration 12
Allen-Bradley PLC Configuration 13
External PLC Configuration 14
External PLC Configuration: Auto-Server Mode (Default) 15
External PLC Configuration: Manual Mode 17
Configuring Read and Write Scan Lines 18
Modbus RTU Slave Configuration 19
Modbus RTU Slave Configuration-Data Groups 20
Modbus RTU Slave Data Group Configuration: Auto-Slave Mode (Default) 21
Modbus RTU Slave Data Group Configuration: Manual Mode 22
Mapping - Transferring Data between Devices 24
Display Mapping and Values 25
Display Data 25
Display String 27
Data and String Mapping – Auto-Map 28
Data Mapping – Explanation 29
Data Mapping – Adding Diagnostic Information 30
String Mapping – Explanation 33
Mapping – Auto-Map Mode to Manual-Map Mode 34
Mapping – Manual-Map Mode to Auto-Map Mode 35
View Data Mapping as Text 36
View String Mapping as Text 37
Security Configuration 38
Security Configuration-Security Levels 39
Security - Log In 40
Security - Log Out 41
Email Configuration 42
Alarm Configuration 43

Diagnostics – Alarm Status 45
Alarms – Active 45
Alarms – Clear 46
Change of State (COS) Configuration 47
Diagnostics Info 48
Diagnostics – Data and String Mapping 48
Diagnostics – Allen-Bradley PLC 49
Diagnostics – Modbus RTU Slave 51
Diagnostics – Modbus RTU Slave 52
LED Configuration 53
Configuration Files 54
Export Configuration 54
Import Configuration 54
Utilities 55
Completing the Installation 56

Overview

The 460ETCMRS gateway connects up to 5 Allen Bradley PLC's to a Modbus RTU Master device. By following this guide, you will be able to configure the 460ETCMRS gateway.

You will set the gateway's network settings, configure device specific parameters for initial operation, and integrate the device into your application.

For further customization and advanced use, please reference the appendices located on the CD. If at any time you need further assistance do not hesitate to call Real Time Automation support.

Support Hours are Monday-Friday 8am-5pm CST

Toll free: 800-249-1612
Email: support@rtaautomation.com

Required Tools and Data

You will need the following tools:

- The gateway
- The provided CD-ROM
    - IPSetup.exe can also be downloaded: http://www.rtaautomation.com/product/460-gateway-support/
- A PC with an internet browser
    - Browser configuration is Firefox / Internet Explorer / Google Chrome compatible
- The supplied Ethernet crossover cable
- A 7-30 VDC power source

Powering The Gateway

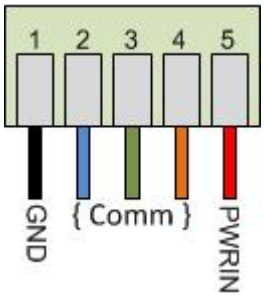
The following steps will allow you to properly and safely power the gateway.

Warning improper wiring will cause unit failure
Use the Barrel Connector OR the Screw Terminals power connection, NOT both

1. Connect a 24VDC power source to the gateway.

   a. The unit draws 125 mA at 24VDC

   b. The gateway has a voltage operating range from 8-30VDC, 24VDC is recommended.



Hazardous Environment Power & Installation Instructions

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D, or non-hazardous locations only.

WARNING – EXPLOSION HAZARD - Do not disconnect equipment unless power has been removed or the area is known to be non-hazardous.

WARNING – EXPLOSION HAZARD - Substitution of components may impair suitability for Class I, Division 2.

THIS EQUIPMENT IS OPEN-TYPE DEVICE AND IS MEANT TO BE INSTALLED IN AN ENCLOSURE SUITABLE FOR THE ENVIRONMENT SUCH THAT THE EQUIPMENT IS ONLY ACCESSIBLE WITH THE USE OF A TOOL.

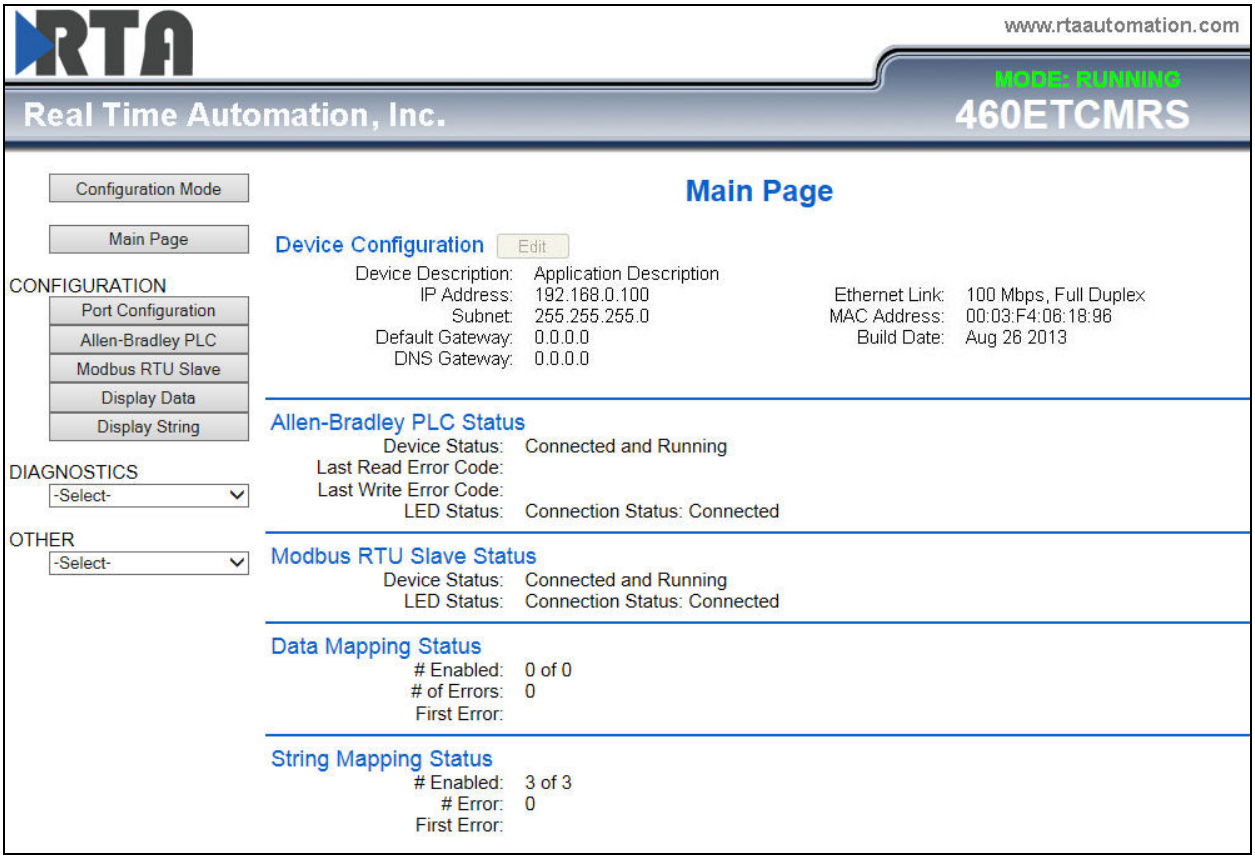
WARNING – POWER JACK (Barrel Connector, J1) IS FOR MAINTENANCE USE ONLY AND MAY ONLY BE USED WHILE THE AREA KNOWN TO BE FREE OF IGNITIBLE CONCENTRATIONS OF FLAMMABLE GASES OR VAPORS. IT IS NOT TO BE CONNECTED UNDER NORMAL OPERATION.

In Hazardous Environments the unit must be powered with between 12-24 VDC, 860 mA (6 W) max. Supervised. The unit is certified to be operated at -40°C to 50°C.

Accessing the Main Page

The following steps will allow you to connect to the browser based configuration of the gateway.

1. Using the supplied crossover cable, connect the gateway to your PC.
2. Insert the provided CD-ROM.
3. Run the IPSetup.exe program from the CD-ROM.
4. Configure the IP Settings of the gateway to be on the same subnet as your PC.
5. Click **Launch Webpage**. The Main page should appear.



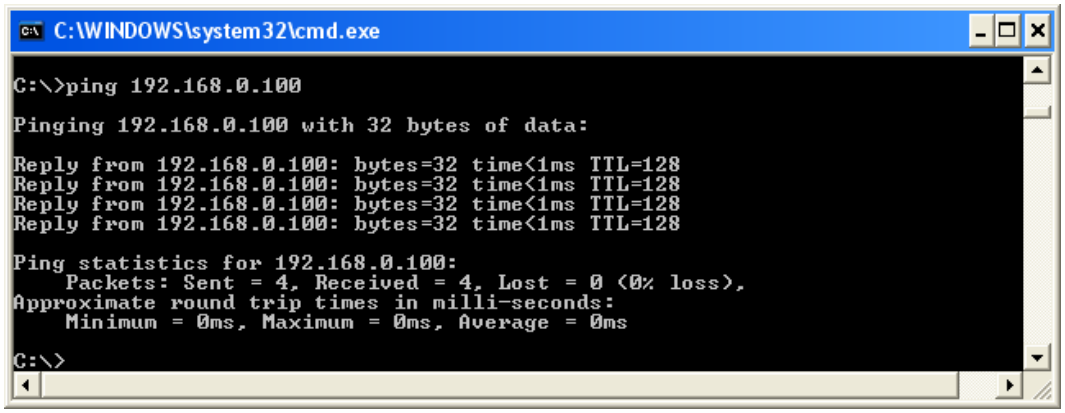
Default IP Address is 192.168.0.100.
Default Subnet is 255.255.255.0.

Error: Main Page Does Not Launch

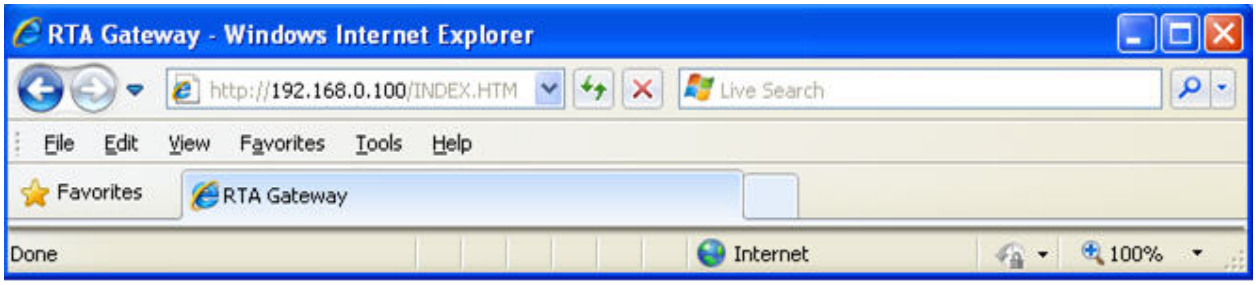
If the Main Page does not launch please verify the following:

1. Check that the PC is set for a Static IP Address
    a. Open a MS-DOS Command Prompt
    b. Type “ipconfig” and press enter
    c. Note the PC’s IP Address, Subnet, and Default Gateway
        i. An invalid IP Address would be: 169.254.x.x
2. The gateway must be on the same Network/Subnet as the PC

Once you have both devices on the same network, you should be able to ping the gateway using a MS-DOS Command Prompt.



If you are able to successfully ping your gateway, open a browser and try to view the main page of the gateway by entering the IP Address of the gateway as the URL.



Main Page

The main page is where important information about your gateway and its connections are displayed.

Mode (orange box below):

Running Mode:

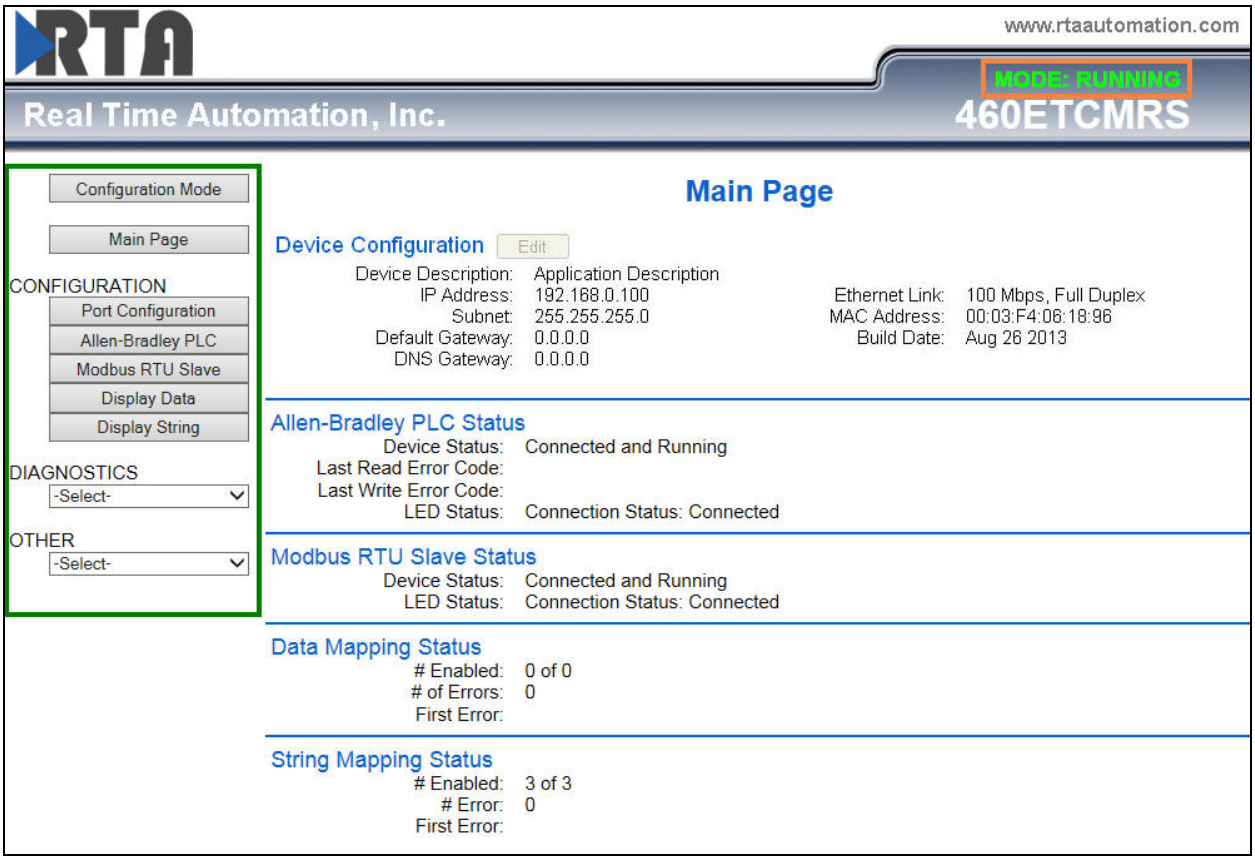
- Protocol communications are enabled
- Configuration cannot be changed during Running Mode. If changes are needed, click the **Configuration Mode** button shown in the green box below

Configuring Mode:

- Protocol communication is stopped and no data is transmitted
- Configuration is allowed

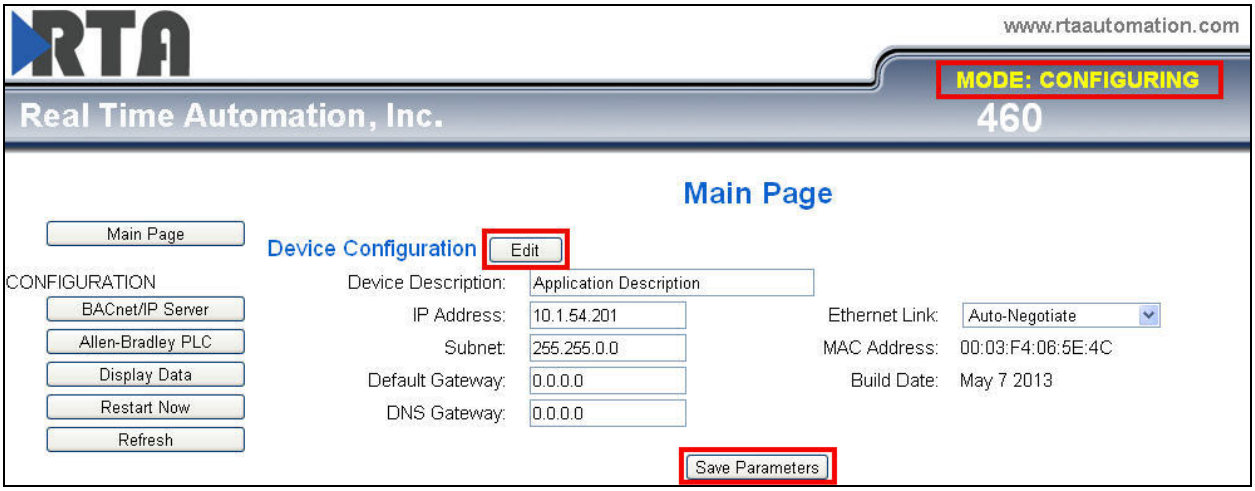
Navigation (green box below):

You can easily switch between modes and navigate between pages (Configuration, Diagnostics, and Other pages) using the buttons on the left hand side.



Device Configuration

The device configuration area is where you assign the device description, IP address, and other network parameters. Changes can only be made when the gateway is in Configuration Mode. Click the **Edit** button to make these changes.



Once you are done configuring the Description and the Network Settings, click the **Save Parameters** button.

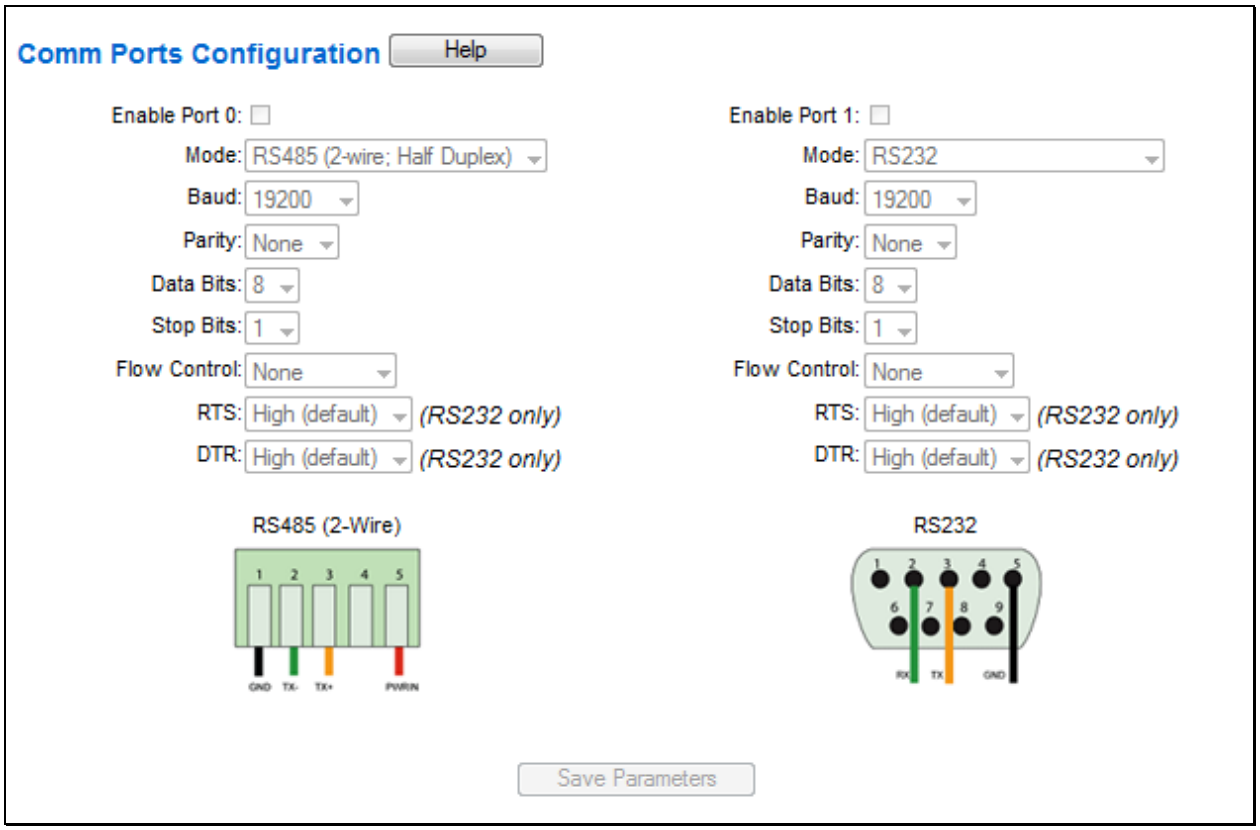
If you are changing the IP Address of the gateway, the change will not take effect until the unit has been rebooted. After reboot, you must enter the new IP Address into the URL.

It is recommended to leave the DNS Gateway set to 0.0.0.0 and the Ethernet Link as Auto-Negotiate. If configuring the gateway to use E-mail, the DNS Gateway must be set.

Port Configuration

The Port Configuration page is where you set port specific parameters. These settings must match the settings of the device(s) that you are connecting to.

When you have completed your port configuration, click the **Save Parameters** button.



The default jumper configurations are setup for the following serial modes:

- **Port 0 - RS485**
- **Port 1 - RS232**

If you require a different serial mode, please refer to the Hardware_Jumper_Configuration.pdf on the CD to make jumper changes.

Allen-Bradley PLC Configuration

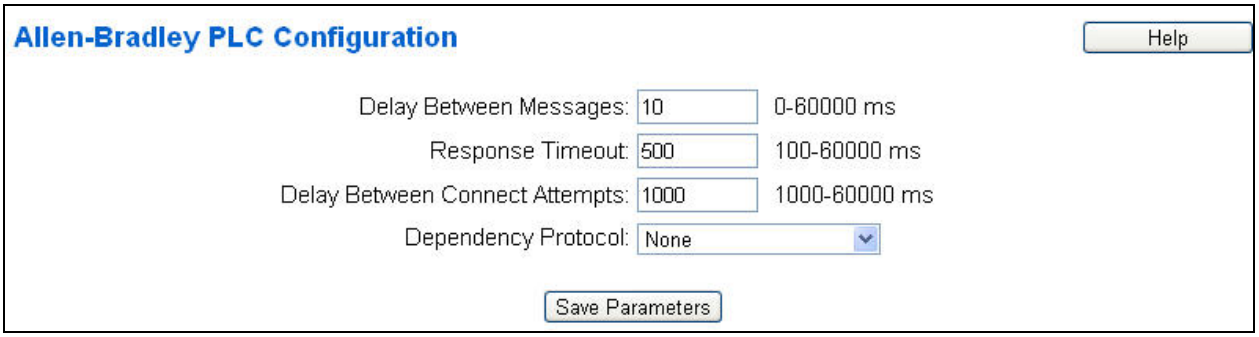
Click the **Allen-Bradley PLC** button to access the configuration page.

1) **Delay Between Messages**: Enter the length of time to delay between read and write scan line requests (ms).

2) **Response Timeout**: Enter the amount of time the gateway should wait before a timeout is issued for a read/write request (ms).

3) **Delay Between Connect Attempts**: Enter the amount of time the gateway should wait between attempts to connect to the PLC.

4) **Dependency Protocol**: If enabled, the Allen-Bradley PLC communication will stop if communication to the selected protocol is lost.



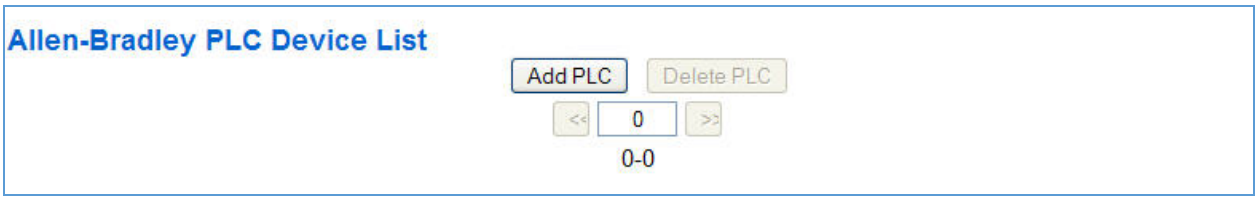
External PLC Configuration

The bottom area of the Allen-Bradley PLC Configuration page lets you configure up to 5 PLCs.

There are two ways to configure this protocol:

- Auto-Server Mode(Default)
- Manual Mode

NOTE: You may go back and forth between modes, but when reverting from Manual Mode to Auto-Server Mode, all changes made in Manual Mode will be discarded.



External PLC Configuration: Auto-Server Mode (Default)

While in Auto-Server mode the # of scan lines and the actual scan lines themselves cannot be edited. Auto-Server Mode looks at the other protocol and then configures the Scan Lines within the PLC to match. The PLC Tag/File Names and Data Types will be defined after the other protocol is configured.

If the PLC is a CompactLogix, ControlLogix, or FlexLogix, the data will be configured according to the following rules:

- Any 8 Bit Signed/Unsigned data will be mapped as **Sint**.
- Any 16 Bit Signed/Unsigned data will be mapped as **Int**.
- Any 32 Bit Signed/Unsigned data will be mapped as **Dint**.
- Any 32 Bit Float and 64 Bit Float data will be mapped as **Real**.
- Any Coils or 1 Bit Binary Packs will be mapped as **Bool (1 Bit**).
- Any Coils or 8/16/32 Bit Binary Packs will be mapped as **Bit Array (32 bit)**.
- Any String Data Types will be mapped as **String**.

If the PLC is a MicroLogix, SLC, or PLC5E, the data will be configured according to the following rules:

- Any 8 Bit Signed/Unsigned and 16 Bit Signed/Unsigned data will be mapped as **Int**.
- Any 32 Bit Signed/Unsigned, 32 Bit Float, and 64 Bit Float data will be mapped as **Real**.
- Any Coils or 1/8/16/32 Bit Binary Packs will be mapped as **Bit Array (16 bit)**.
- Any String Data Types will be mapped as **String**.

Regardless of PLC type, the following is also true:

- The Read or Write direction depends on whether it is configured as a Read or Write on the other protocol.
- If the other protocol exceeds the number of Sint, Int, Dint, Real, Bool, Bit Array, or String Data Types the Allen-Bradley PLC supports (see limits on webpage), then nothing will be mapped. You will see the # of Scan Lines remain at 0 and the main page will display the following error:

  - To fix this error, simply decrease the amount of data you configured on the other protocol so that the max number of Tag/File Name is not exceeded OR call customer support to increase the limits.

1. For additional PLC's, click the **Add PLC** button and follow instructions under Manual Mode for each additional device.

   -Auto-Server Mode only affects PLC 1.

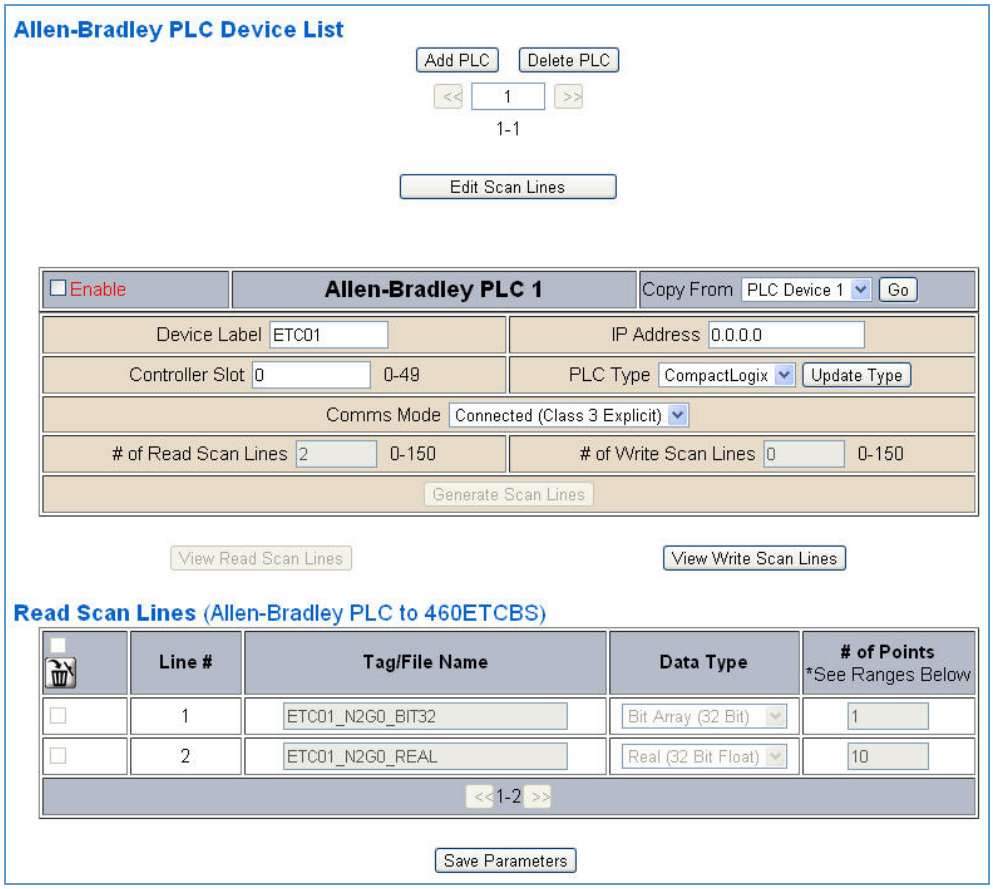
2. The **Enable** check box should be selected for the device.

3. Enter a **Device Label** to identify the device within the gateway.

4. Enter the **IP Address** of the PLC, the **Controller Slot** (Integrated Ethernet, use Slot 0), and select the **PLC Type**. The Controller Slot is the slot where the Controller is located, not the Ethernet Card being used. These 3 parameters must match the PLC you are communicating to.

5. Select the **Comms Mode**. Unconnected (UCMM) messaging relies on shared resources to transfer data to/from the PLC. This could result in message timeouts if there are a lot of devices fighting for these shared buffers. Connected (Class 3 Explicit) messaging relies on reserved resources to transfer data to/from the PLC. RTA recommends using Connected.

6. To edit scan lines, you will need to go into Manual Mode.



External PLC Configuration: Manual Mode

1. Click the **Edit Scan Lines** button to switch from Auto-Server Mode to Manual Mode. Once clicked the button will read **Auto-Configure PLC**. The fields under the Scan Lines can now be edited.

    a. When prompted, click **OK** to confirm mode change or **Cancel** to remain in Auto Mode.

    b. Click **OK** again to keep current Scan Line settings or click **Cancel** to discard the current configuration.

2. For additional PLC's, click the **Add PLC** button.

    -To remove a device, click the **Delete PLC** button.

    - To copy parameters from a device you have already configured, select the device you wish to copy parameters from in the **Copy From** dropdown menu. Then, click the **Go** button. Once copied, you can make any changes needed to the device you are adding.

3. The **Enable** check box should be selected for the device.

4. Enter a **Device Label** to identify the device within the gateway.

5. Enter the **IP Address** of the PLC, the **Controller Slot** (Integrated Ethernet, use Slot 0), and select the **PLC Type**. The Controller Slot is the slot where the Controller is located, not the Ethernet Card being used. These 3 parameters must match the PLC you are communicating to.

6. Select the **Comms Mode**. Unconnected (UCMM) messaging relies on shared resources to transfer data to/from the PLC. This could result in message timeouts if there are a lot of devices fighting for these shared buffers. Connected (Class 3 Explicit) messaging relies on reserved resources to transfer data to/from the PLC. Connected messaging is recommended.

7. Enter the number of Read Scan Lines and Write Scan Lines.

8. Click **Generate Scan Lines** to have the read and write scan lines auto-generated for you. If you need to manually configure the read and write scan lines you can do so after they have been generated.

Configuring Read and Write Scan Lines

Follow these steps to manually configure Read and Write Scan Lines.

1) Click the **View Read Scan Lines** or **View Write Scan Lines** button.

2) Enter the **Tag/File Name** that is set up within the PLC. This Tag/FileName must exist at the Controller Scope - not the Program Scope.

   -If you wish to start from a point other than the base, add [#] to the end of the Tag/File Name to specify which point is the starting point.

   Example: A tag called "ReadTag" has dimension of 100 in the PLC. By default, we will start at point 0 of that array. Therefore, "ReadTag" and "ReadTag[0]" refer to the same point. To start from a different point, such as array index 27, enter in "ReadTag[27]" as the Tag/File Name in our gateways scan line. This means the gateway will go to "ReadTag" and start at array index 27.

   -If you wish to access a specific bit from any Data Type, you must use the Mapping Page's Set Bit math function. *You may **not** use ReadTag/0.0 to access bits.*

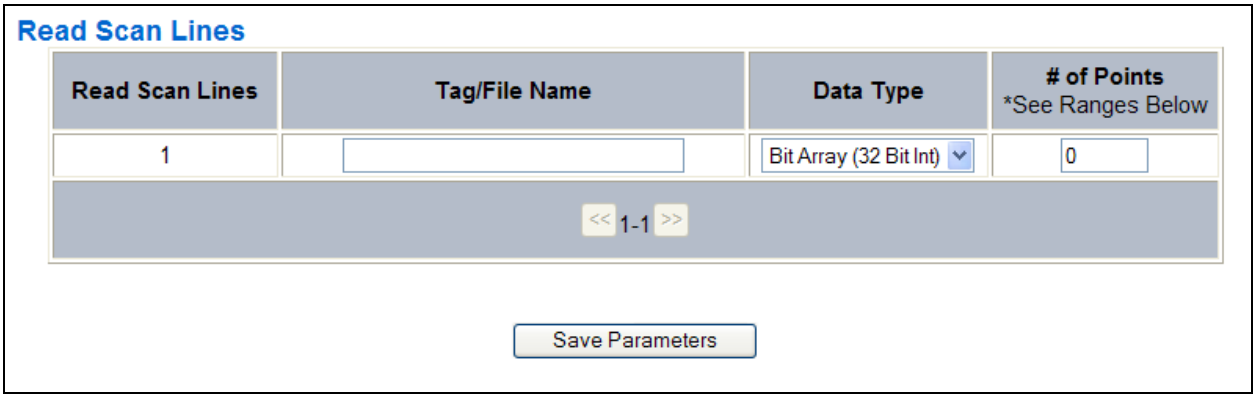
3) Select the **Data Type** of the Tag/File.

4) Enter the **# of Points** you want to move from the PLC Tag/File to the gateway. See the *Scan Line Data Limit* section at the bottom of the page for the given max values.

   -Example continued: Consider # of points is set to 10. If tag is set as "ReadTag" or "ReadTag[0]" this will read in array points 0 through 9. If tag is set as "ReadTag[27]" this will read in array points 27 through 36.

5) Click the **Save Parameters** button.

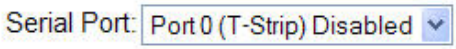
6) Repeat for the other direction if needed.



Modbus RTU Slave Configuration

Click the **Modbus RTU Slave** button to access the configuration page.

1) **Serial Port**: Select which serial port is being used for communication. This port must be configured on the Port Configuration page. If it has not yet been configured, it will display *Disabled* after the Port descriptions in this dropdown.



2) Enter a **Device Label** to identify the device within the gateway.

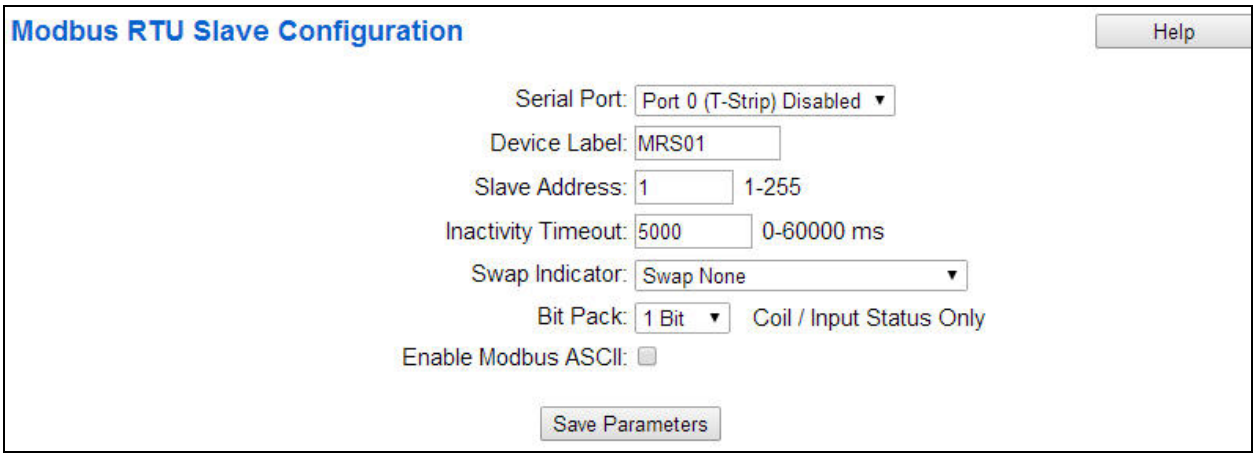
3) **Slave Address**: This Slave Address must be unique for all Modbus RTU Slave devices on the RS485 network.

4) **Inactivity Timeout**: Amount of time the gateway will wait for a Read/Write request before issuing a timeout.

5) To enable data swapping, select the required **Swap Indicator**. If the bytes appear in the wrong order, enable swapping to change the data. This swapping does *NOT* change Coils and their ordering inside the Bit Pack.

6) **Bit Pack**: Select the formatting of the Coil Status/Input Status. Automap will use this packing size to map coils to/from the other protocol. The bit pack selection here should match that of the other protocol. The starting address is considered Bit 0 and is the low-order bit.

7) **Enable Modbus ASCII**: Enable ONLY if you want to communicate using Modbus ASCII. The Master must support Modbus ASCII.



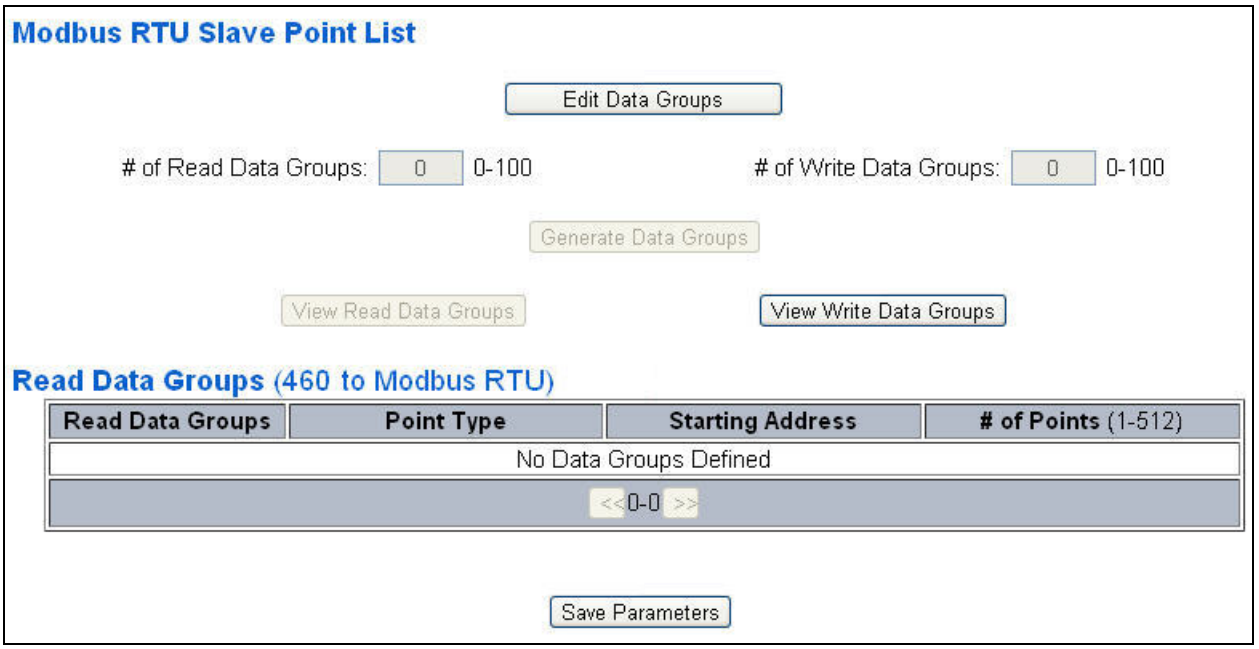
Modbus RTU Slave Configuration-Data Groups

The bottom area of the Modbus RTU Slave Configuration page lets you configure up to 100 Data Groups for both Read/Write.

There are two ways to configure this protocol:

- Auto-Slave Mode(Default)
- Manual Mode

NOTE: You may go back and forth between modes, but when reverting from Manual Mode to Auto-Slave Mode, all changes made in Manual Mode will be discarded.



Modbus RTU Slave Data Group Configuration: Auto-Slave Mode (Default)

While in Auto-Slave mode the # of data groups and the actual data groups themselves cannot be edited. Auto-Slave Mode looks at the other protocol and then configures the Data Groups to match. The Data Formats will be defined after the other protocol is configured.

The data will be configured according to the following rules:

- Any Coils, 8 Bit Signed/Unsigned, or 1/8/16/32 Bit Binary Packs data will be mapped as **0x Coil Status.**
- Any 16 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 16 Bit Int or 16 Bit Uint**, matching signs whenever possible.
- Any 32 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 32 Bit Int or 32 Bit Uint**, matching signs whenever possible.
- Any 64 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 64 Bit Int or 64 Bit Uint**, matching signs whenever possible.
- Any 32 Bit Float will be mapped as **4x Hold Reg 32 Bit Float**.
- Any 64 Bit Float will be mapped as **4x Hold Reg 64 Bit Float**.
- Any String Data Types will be mapped as **4x Hold Reg String**.
- The Read or Write direction depends on whether it is configured as a Read or Write on the other protocol.
- If the other protocol exceeds the number of Data Groups supported, then nothing will be mapped. You will see the # of Data Groups remain at 0 and the main page will display the following error:

  - To fix this error, simply decrease the amount of data you configured on the other protocol so that the max number of Data Groups is not exceeded OR call customer support to increase the limits.

To add additional or edit existing Data Groups you will need to go into Manual Mode.

Modbus RTU Slave Data Group Configuration: Manual Mode

1. Click the **Edit Data Groups** button to switch from Auto-Slave Mode to Manual Mode. Once clicked the button will read **Auto-Configure Slave**. The fields under the Data Groups can now be edited.

    a. When prompted, click **OK** to confirm mode change or **Cancel** to remain in Auto Mode.

    b. Click **OK** again to keep current Data Group settings or click **Cancel** to discard the current configuration.

2. Enter the number of Read Data Groups and Write Data groups.

3. Click the **Generate Data Groups** button to have the Read and Write data groups auto-generate for you. You may manually configure the Read and Write data groups after they have been generated.

4. Follow these steps to manually configure Read Data Groups.

    a. Select **View Read Data Groups** if not already selected.

    b. Select a **Point Type** for each Scan Line. Options include: Coil Status, Input Status, Input Registers, and Holding Registers. **Note**: Input/Holding Registers have a data type associated with them.

        - String Point Type- If the mating protocol supports strings, you may select string as a point type in Modbus. With this point type, 2 characters will be packed into a single register and the first register will be set aside for the length.

          EX: 4x Hold Reg (String) with a Starting Address of 1 for a length of 5 Registers

          This means that Register 1 will hold the length of the string and Registers 2-5 will hold the string contents. This string can contain a max of 8 characters.

    c. Enter a **Starting Address** (1-based).

    d. Enter the **# of Points** to read. This will allocate the number of the data type selected.

5. Follow these steps to manually configure Write Data Groups.

    a. Select **View Write Data Groups** if not already selected.

    b. Select a **Point Type** to configure. Options include: Coil Status and Holding Registers. **Note**: Holding Registers have a data type associated with them.

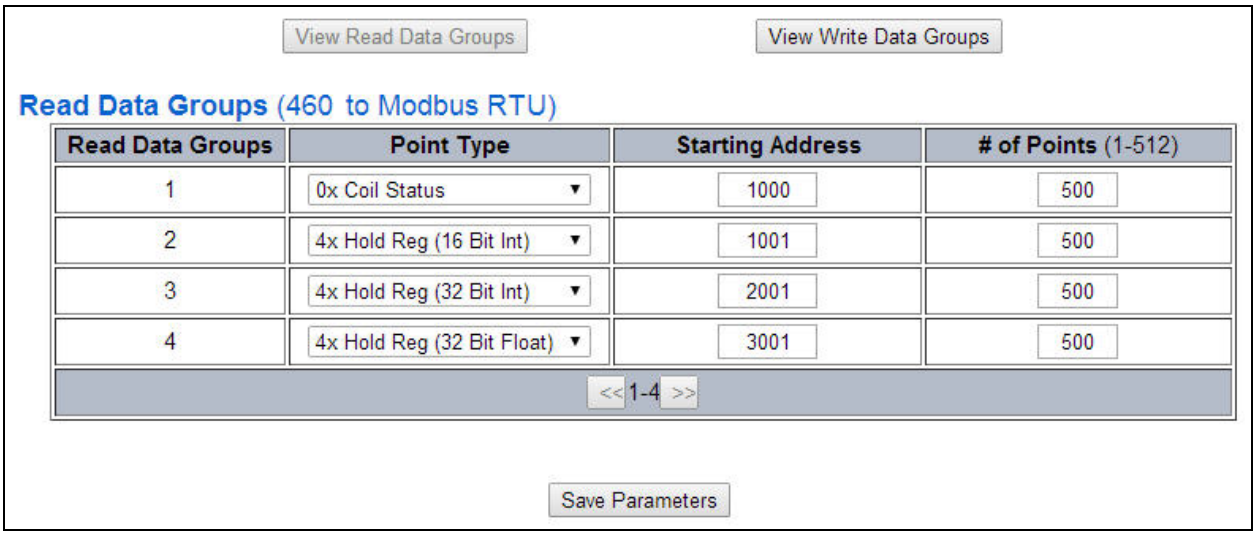
        - String Point Type- If the mating protocol supports strings, you may select string as a point type in Modbus. With this point type, 2 characters will be packed into a single register and the first register will be set aside for the length.

EX: 4x Hold Reg (String) with a Starting Address of 1 for a length of 5 Registers

This means that Register 1 will hold the length of the string and Registers 2-5 will hold the string contents. This string can contain a max of 8 characters.

c. Enter a **Starting Address** (1-based).

d. Enter the **# of Points** to write. This will allocate the number of the data type selected.



Mapping - Transferring Data between Devices

There are 5 ways to move data from one protocol to the other. You can combine any of the following options to customize your gateway as needed.

Option 1 – Data Auto-Map: The gateway will automatically take the data type (excluding strings) from one protocol and look for the same data type defined in the other protocol. If there isn't a matching data type, the gateway will map the data to the largest available data type. See Data Auto-Map section for more details.

Option 2 – String Auto-Map: The gateway will automatically take the string data type from one protocol and map it into the other. See String Auto-Map section for more details.

Option 3 – Manual Map: If you don't want to use the Auto-Map function, you must use the manual mapping feature to configure translations.

Option 4 – Manipulation/Scaling: You can customize your data by using math operations, scaling, or bit manipulation. See Data Mapping-Explanation section for more details.

Option 5 – Move Diagnostic Information: You can manually move diagnostic information from the gateway to either protocol. Diagnostic Information is not mapped in Auto-Map mode. See Diagnostic Info section for more details.

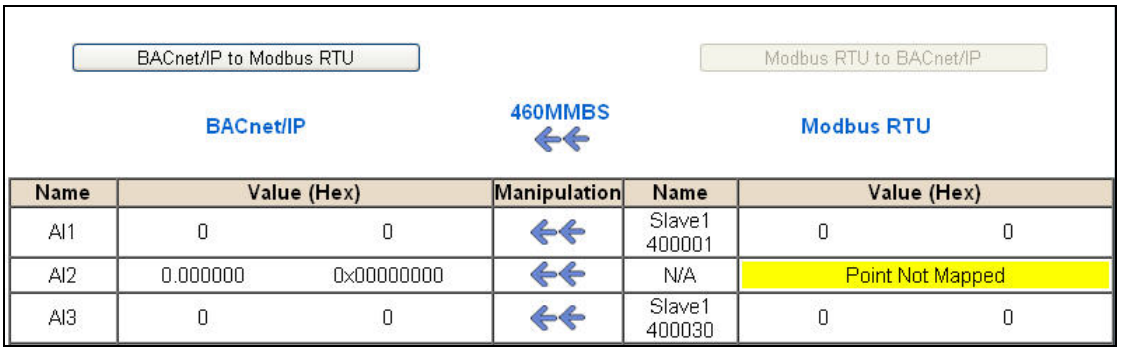
Display Mapping and Values

The Display Data and Display String pages are where you can view the actual data for each mapping that is set up.

Display Data

Click the **Display Data** button to view how the data is mapped and what the values of each mapping are. Here you will see how each data point (excluding strings) is mapped. To view, select the device from the dropdown menu and click **View** to generate the information regarding that device. Then select either the ***Protocol 1 to Protocol 2*** or ***Protocol 2 to Protocol 1*** button, correlating to the direction you wish to see the data.

This page is very useful when verifying that all data is mapped somehow from one protocol to another. If a data point is not mapped, it will display on this page in a yellow highlighted box.



Name	Value (Hex)		Manipulation	Name	Value (Hex)	
AI1	0	0	⇐⇐	Slave1 400001	0	0
AI2	0.000000	0x00000000	⇐⇐	N/A	Point Not Mapped	
AI3	0	0	⇐⇐	Slave1 400030	0	0

In the above example, we see the following:

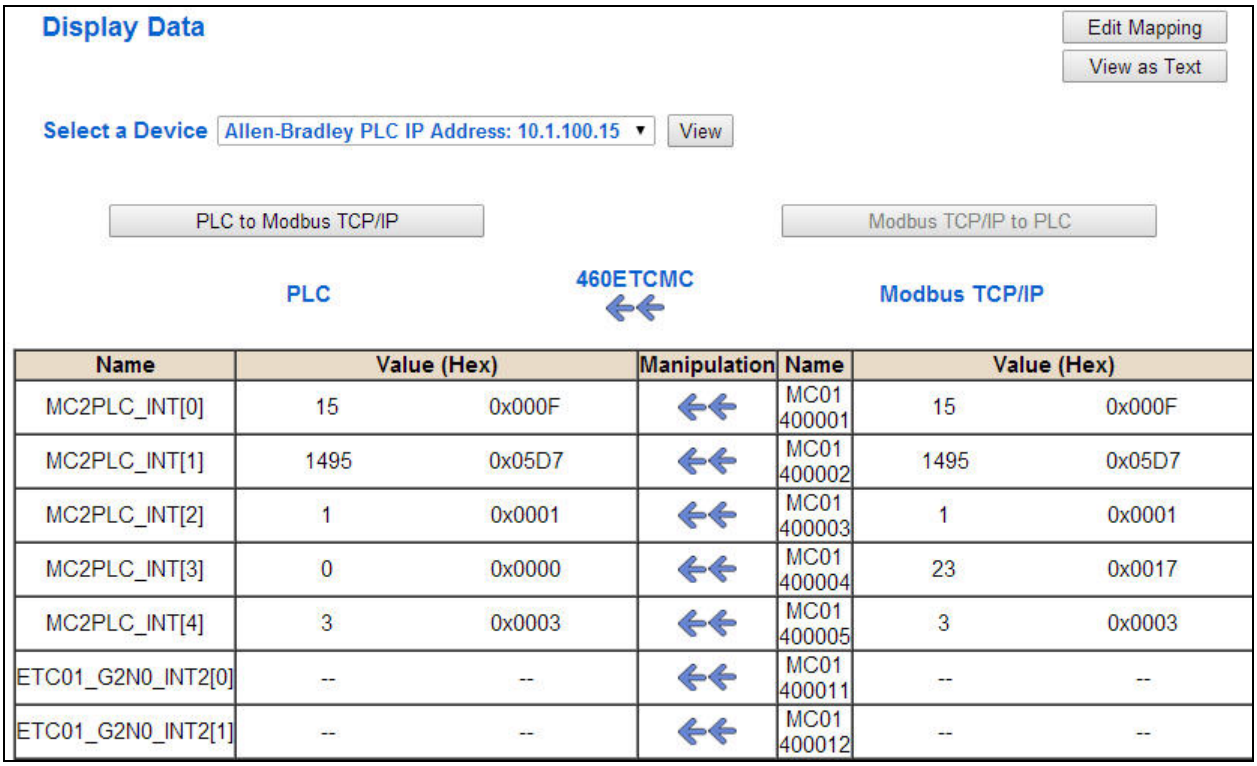
- Modbus 400001 from Slave 1 is being mapped to AI1 on BACnet
- Nothing is being moved from Modbus to AI2 on BACnet
- Modbus 400030 from Slave 1 is being mapped to AI3 on BACnet

NOTE: If a data point is mapped twice, only the first instance of it will show here. EX: If Modbus 400001 & 400040 from Slave 1 are both mapped to AI1, only 400001 will show as being mapped to AI1.

If there are values of "- -" on this page, it indicates that the source has not yet been validated and no data is being sent to the destination.

The example below reflects the Modbus to PLC flow of data. The Modbus (right side) is the source and the PLC (left side) is the destination.

- The 460 gateway has received valid responses from Modbus registers 400001-400005 and therefore can pass the data on to the PLC tag called MC2PLC_INT.
- The 460 gateway has NOT received valid responses from Modbus register 400011 & 400012. As a result, the data cannot be passed to the PLC tag ETC01_GN0_INT2 and indicates so by using "- -" in the value column of the table.



Name	Value (Hex)		Manipulation	Name	Value (Hex)	
MC2PLC_INT[0]	15	0x000F	←	MC01 400001	15	0x000F
MC2PLC_INT[1]	1495	0x05D7	←	MC01 400002	1495	0x05D7
MC2PLC_INT[2]	1	0x0001	←	MC01 400003	1	0x0001
MC2PLC_INT[3]	0	0x0000	←	MC01 400004	23	0x0017
MC2PLC_INT[4]	3	0x0003	←	MC01 400005	3	0x0003
ETC01_G2N0_INT2[0]	--	--	←	MC01 400011	--	--
ETC01_G2N0_INT2[1]	--	--	←	MC01 400012	--	--

To view the actual data mappings, click the **Edit Mapping** button. For more details, see the Data Mapping-Explanation section.

To view the data mappings purely as text, click the **View as Text** button. For more details, see the View Data Mapping as Text section.

Display String

Click the **Display String** button to view how the string data types are mapped and what the values of each string are. Here you will see how each string from each protocol is mapped to the other. To view, select the source or destination group and the String from the dropdown menu to generate the information regarding that device. The string data will be displayed in both hex and ASCII.

If there are values of “Data Not Valid“ on this page, it indicates that the source has not been validated yet and no data is being sent to the destination.

In the example below, this page reflects the Modbus to PLC flow of data. Since the Destination “Dst: ETC01 ETC01_G2N0_STRING” displays “Data Not Valid”, it can be assumed that the source field has not yet been validated.

To view the string mappings, click the **Edit Mapping** button. For more details see the String Mapping-Explanation section.

To view the string mappings purely as text, click the **View as Text** button. For more details see the View String Mapping as Text section.

Data and String Mapping – Auto-Map

The Auto-Map function looks at both of the protocols and will map the data between the two protocols as best as it can so that all data is mapped. Inputs of like data types will map to outputs of the other protocols like data types first. If a matching data type cannot be found, then the largest available data type will be used. Only when there is no other option is data truncated and mapped into a smaller data type.

If the Auto-Map function does not map the data as you want or you want to add/modify the mappings, you may do so by going into Manual-Map mode.

The following are examples of the Auto-Map function.

1) This example shows a common valid setup.

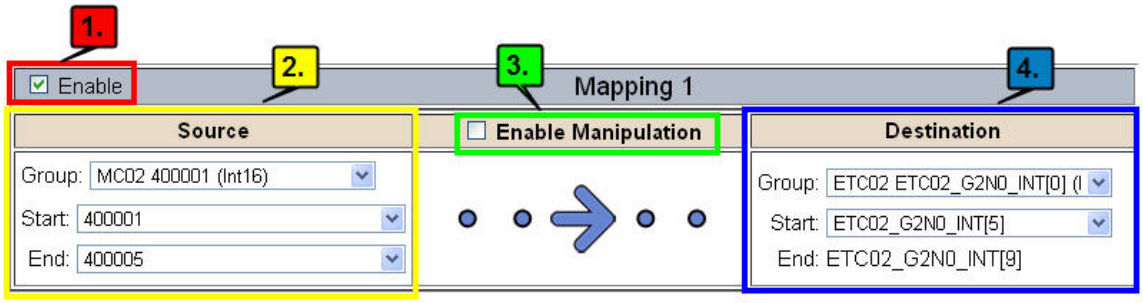
   a. Both Source values were able to be mapped to a corresponding Destination value.

2) This example shows how Auto-Map will make its best guess.

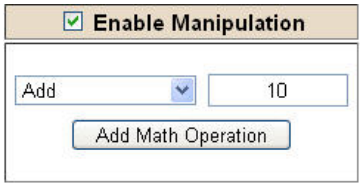
   a. The 32-bit Float from the Source location could not find a matching Destination data-type. After all other like data types were mapped, the only data type available was the 2nd 32-bit Uint data type. Auto-Map was completed even though the data in the Float will be truncated.

Data Mapping – Explanation

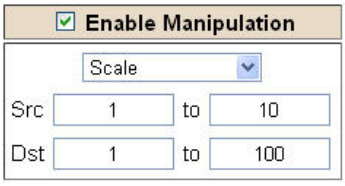
Below are the different parts that can be modified to make up a data mapping.



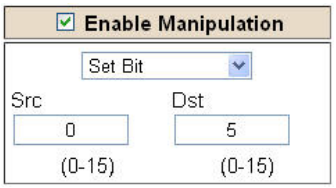
1. Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2. Source Field (yellow box above) :
    a. Group - Select the data group you set up in the protocol config to use for this mapping.
    b. Start - This is the starting point for this mapping.
    c. End - This is the final point to be included for this mapping.
3. Manipulation Area (green box above) :
    a. Enable the Data Manipulation. This can be enabled for any mapping.
    b. Click **Add Math Operation** for each operation needed. Up to 3 are allowed unless you are using the Scale, Set Bit, or Invert Bit functions. If using Scale, Set Bit, or Invert Bit, then only 1 operation is allowed.
    c. Select the Operation(s) to perform.
        i. Math Operations are preformed in the order they are selected.
        ii. If more than one point is selected on the source, the Math Operations will be performed on every point.
    d. Enter the value(s) for the operation.



Example of Add (similar for Subtract, Multiple, Divide, and MOD). This will add a value of 10 to the source field before it is written to the destination field.



Example of Scale. This will scale the source values from 1-10 into 1-100 for the destination.



Example of Set Bit (similar to Invert Bit). This will take the value of the 0th source bit and copy it into the value of the 5th destination bit.

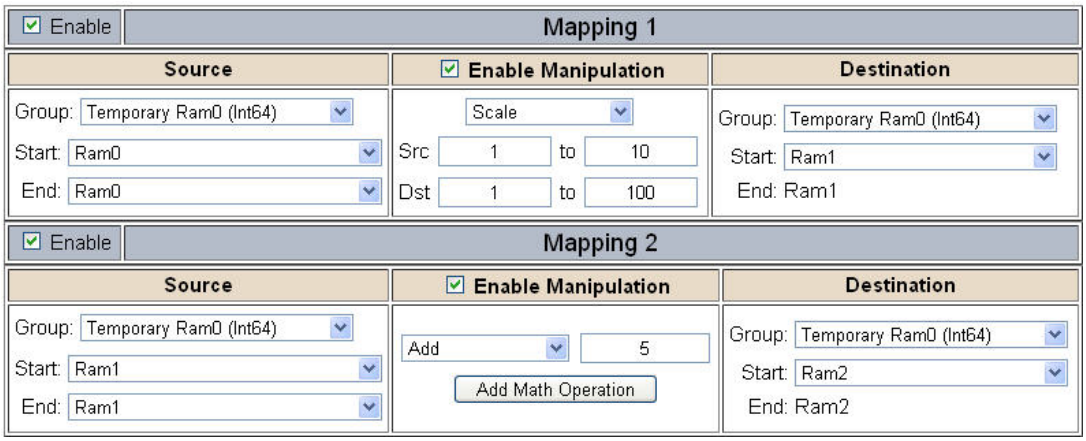
4. Destination Field (blue box above) :
    a. Group - Select the data group you set up in the protocol config to use for this mapping.
    b. Start - This is the starting point for where the data is being stored.
    c. End - The End point is derived from the length of the source and cannot be modified.

Data Mapping – Adding Diagnostic Information

Data Mapping offers 5 different types of information in addition to any scan lines specified for each protocol.

IMPORTANT NOTE: Only add Diagnostic Information **AFTER** both sides of the gateway have been configured. If changes to either protocol are made after diagnostic information has been added to the mapping table, it is necessary to verify all mappings. Remapping may be necessary.

1. Temporary Ram (Int 64)
    a. This offers five levels of 64bit Integer space to assist in multiple stages of math operations. For example, you may wish to scale and then add 5. You can set up a single translation to scale with the destination as the temporary ram. Then another translation to add 5 with the source as the temporary ram.
    b. The gateway will automatically convert the Source to fit the Destination, so there is no need for Int 8, 16, 32 since the 64 may be used for any case.



In this example, Ram0 is scaled into Ram1. Ram1 is then increased by 5 and stored into Ram2. Ram0 and Ram2 could be considered a source or destination group.

2. Temporary Ram (Double)
    a. This is similar to the Temporary Ram (Int 64), except manipulations will be conducted against the 64bit floating point to allow for large data.
3. Ticks Per Second
    a. The gateway operates at 200 ticks per second. This equates to one tick every 5ms. Thus, mapping this to a destination will give easy confirmation of data flow without involving one of the two protocols.
4. XY_NetBmpStat
    a. If a protocol is a Client/Master, there is a Network Bitmap Status that is provided. Since a Client/Master may be trying to communicate with multiple devices on the network, it

may be beneficial to know if a Server/Slave device is down. By using this Network Bitmap Status you can expose the connection statuses of individual devices.

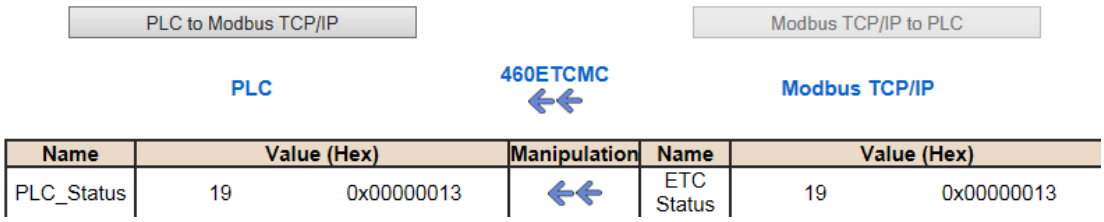
b. 0x00000002 shows that only device 2 is connected
c. 0x00000003 shows that only devices 1 and 2 are connected
d. 0x00000004 shows that only device 3 is connected

5. Status_XY
   a. There are two Statuses provided, one for each protocol. This gives access to the overall status of that Protocol. Each Bit has its own meaning as follows:

Common Status: 0x000000FF (bit 0-7)1st byte

Hex:	Bit Position:	Decimal:	Explanation:
0x00	0	0	if we are a Slave/Server
0x01	0	1	if we are a Master/Client
0x02	1	2	connected (0 not connected)
0x04	2	4	first time scan
0x08	3	8	idle (usually added to connected)
0x10	4	16	running (usually added to connected)
0x20	5	32	bit not used
0x40	6	64	recoverable fault
0x80	7	128	nonrecoverable fault

For this example the ETC Status is mapped to a PLC tag called PLC_Status



Example: ETC Status is 0x00000013 (19 decimal), here is the break down

Hex	Bit	Decimal	Explanation
0x01	0(on)	1	if we are a Master/Client
0x02	1(on)	2	connected (0 not connected)
0x10	4(on)	16	running (usually added to connected)
Total: 0x13		19	

External Faults: 0x0000FF00 (bit 8-15)2nd byte

Hex:	Bit Position:	Decimal:	Explanation:
0x00	8	0	local control
0x01	8	256	remotely idle
0x02	9	512	remotely faulted
0x04	10	1,024	idle due to dependency
0x08	11	2,048	faulted due to dependency

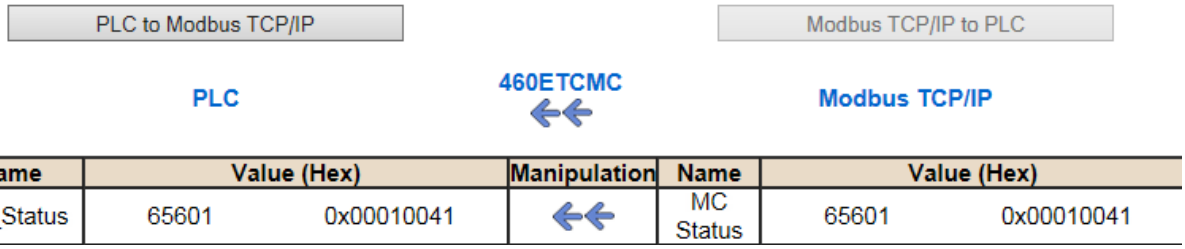
Recoverable Faults: 0x00FF0000 (bit 16-23)3rd byte

Hex:	Bit Position:	Decimal:	Explanation:
0x01	16	65,536	recoverable fault - timed out
0x02	17	131,072	recoverable fault - Slave err

Non-Recoverable Faults 0xFF000000 (bit 24-31)4th byte

Hex:	Bit Position:	Decimal:	Explanation:
0x01	24	16,777,216	nonrecoverable fault – task fatal err
0x02	25	33,554,432	nonrecoverable fault – config missing
0x04	26	67,108,864	nonrecoverable fault – bad hardware port
0x08	27	134,217,728	nonrecoverable fault – config err
0x10	28	268,435,456	Configuration Mode
0x20	29	536,870,912	No Ethernet Cable Plugged In

For this example the MC Status is mapped to a PLC tag called MC_Status



Name	Value (Hex)		Manipulation	Name	Value (Hex)	
MC_Status	65601	0x00010041		MC Status	65601	0x00010041

Example: MC Status is 0x00010041 (65601 decimal), here is the break down, we know that bytes 1 and 3 are being used, so here is the break down,

Common Status:

Hex:	Bit:	Decimal:	Explanation:
0x01	0(on)	1	if we are a Master/Client
0x40	6(on)	64	recoverable fault

Recoverable Faults:

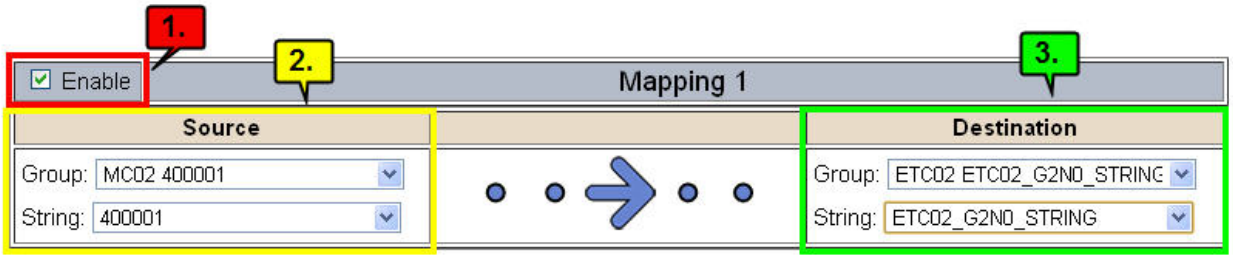
Hex:	Bit:	Decimal:	Explanation:
0x01	16	65,536	recoverable fault – timed

Total:	0x010041	65,601

String Mapping – Explanation

Below are the different parts that can be modified to make up a string mapping.

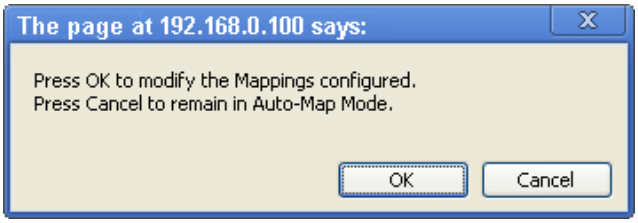
String data types can only be mapped to other string data types. There is no manipulation that can be done on the string.



1. Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2. Source Field (yellow box above) :
    a. Group - Select the string data group you set up in the protocol config to use for this mapping.
    b. String - This is the string used for this mapping.
3. Destination Field (green box above):
    a. Group - Select the string data group you set up in the protocol config to use for this mapping.
    b. String - This is the string where the data is being stored.

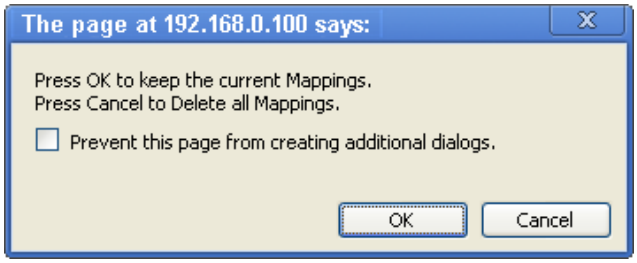
Mapping – Auto-Map Mode to Manual-Map Mode

To transition from Auto-Map mode to Manual-Map mode, click the **Edit Mapping** button. After you click this button, you will be prompted to confirm if this is really what you want to do.



Click **OK** to proceed to Manual Map mode or click **Cancel** to remain in Auto-Map mode.

There are 2 options on how to proceed from here.

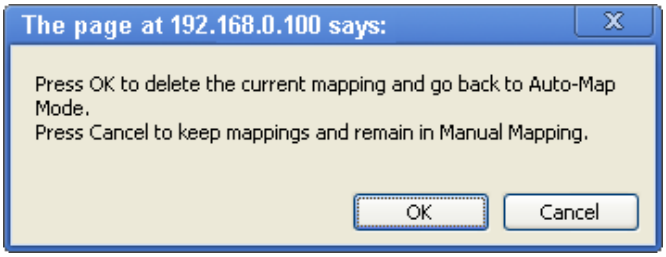

The page at 192.168.0.100 says:
Press OK to keep the current Mappings.
Press Cancel to Delete all Mappings.
Prevent this page from creating additional dialogs.
OK
Cancel

1) To keep the mappings that are already configured press **OK**.
    a. You would want this option if you are adding additional mappings or you want to modify the mapping(s) that already exist.
2) To delete the mappings that are already there and start over press **Cancel**.

To modify the number of mappings, enter a number next to **# of Mappings to Configure** and click the **Set Max # of Mappings** button. You can always add more mappings if needed.

Mapping – Manual-Map Mode to Auto-Map Mode

To transition from Manual-Map mode to Auto-Map mode, click the **Auto Map Mode** button. After you click this button, you will be prompted to confirm if this is really what you want to do.


The page at 192.168.0.100 says:
Press OK to delete the current mapping and go back to Auto-Map Mode.
Press Cancel to keep mappings and remain in Manual Mapping.
OK
Cancel

Click **OK** to proceed to delete all current mappings and go to Auto-Map mode. Click **Cancel** to keep all mappings and remain in Manual-Map mode.

NOTE: Once you revert back to Auto-Map mode there is no way to recover the mappings you lost. Any mappings you added will be deleted as well.

View Data Mapping as Text

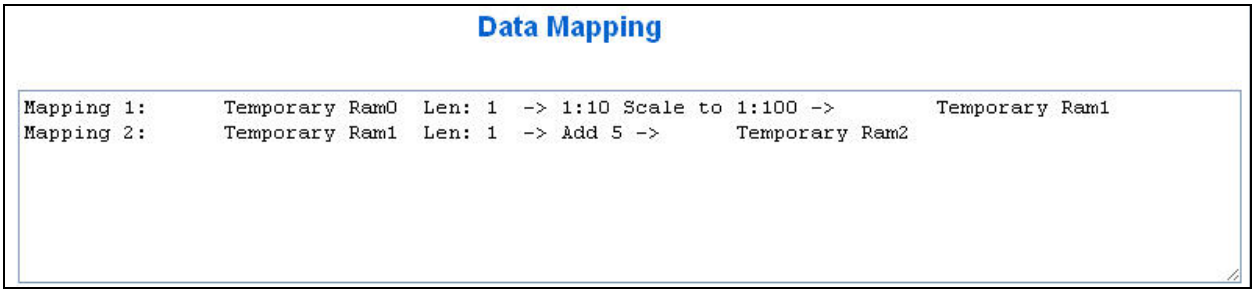
The View as Text page displays the point to point mapping(s) you set up in the Data Mapping section. This will also display any manipulation(s) that are configured.

Each line on this page will read as follows:

> **Mapping** *number***:** *source point* **Len:** *Number of points mapped* **->** *manipulation (if blank then no manipulation)* **->** *destination point*

If you are looking for a specific point to see if it is mapped, you can do a find in this text box for your point in question. Example: you defined 20 Registers starting at register 1 and want to see if 400011 is mapped. If it is not in this text box then it is not mapped and no data will be transferred.

This is the text display for the example shown under the *Data Mapping- Adding Diagnostic Information* section.


Data Mapping
Mapping 1: Temporary Ram0 Len: 1 -> 1:10 Scale to 1:100 -> Temporary Ram1
Mapping 2: Temporary Ram1 Len: 1 -> Add 5 -> Temporary Ram2

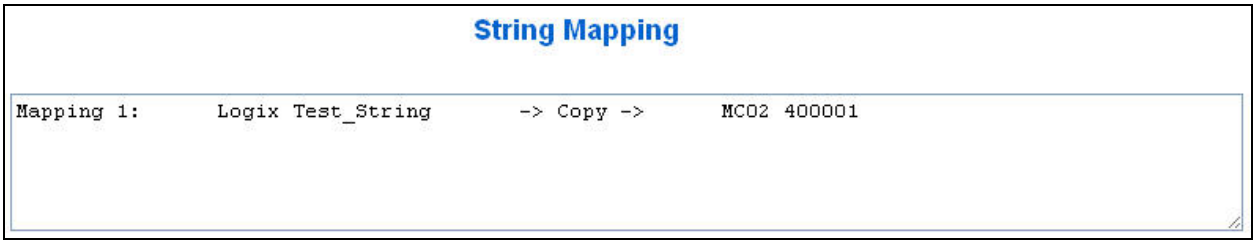
View String Mapping as Text

The View as Text page displays the string mapping(s) you set up in the String Mapping section.

Each line on this page will read as follows:

Mapping *number***:** *source point* **-> Copy ->** *destination point*

If you are looking for a specific point to see if it is mapped, you can do a find in this text box for your point in question. Example: you defined 20 String Tags in the PLC and want to see if "Test_String" in the Logix PLC is mapped. If it is not in this text box, then it is not mapped, and no data will be transferred.



Security Configuration

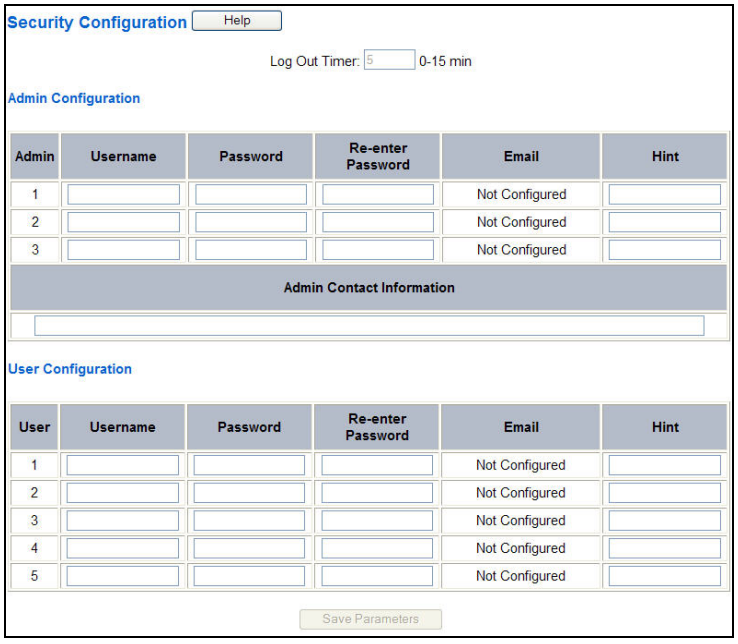
You can configure Security for 3 administrators, 5 users, and 1 guest.

THIS IS NOT A TOTAL SECURITY FEATURE

The security feature offers a way to password protect access to diagnostics and configuration on the network. The security feature does not protect against "Air Gap" threats. If the gateway can be physically accessed, security can be reset. All security can be disabled if physical contact can be made. From the login page, you would click the **Reset Password** button twice and be forced to do a hard reboot (power down) on the gateway within 15 minutes of clicking the button. This process should be used in the event a password is forgotten.

Note: Only Admins have configuration access to all web pages.

1. Log Out Timer: The system will automatically log inactive users off after this period of time.
2. Username: Enter a username, max of 32 characters.
3. Password: Enter a password for the username, max of 32 characters, case sensitive.
    a. Re-enter the Password
4. E-mail: In case the password was forgotten, a user can have their password e-mailed to them if e-mail was configured.
5. Hint: A helpful reminder of what the password is.



Security Configuration-Security Levels

Each webpage in our gateway can have a separate security level associated with it for each user.

Security Levels:

1. **Full Access**: Capability to view and configure a web page.
2. **View Access**: Capability to view a web page, but cannot configure parameters.
3. **No Access**: No capability of viewing the web page and page will be removed from Navigation.

Security - Log In

Username: Name of the user to login.

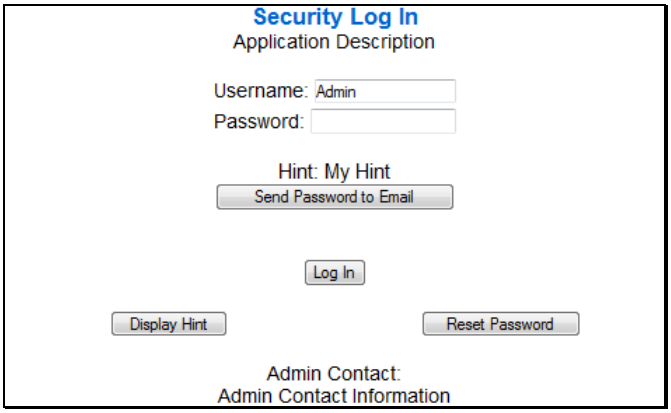
Password: Password of the user to login.

Log In: If login is successful, the user will be redirected to the Main Page.

Send Password to Email: Sends the specified User's Password to the email configured for that user.

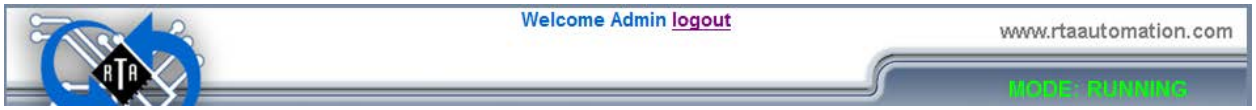
Display Hint: Displays the hint specified for the User if one was set up.

Reset Password: This is used to reset security settings. Confirm reset password must be selected to confirm this action. Once confirmed, there is a 15 minute window to do a hard reset of the gateway by physically removing and restoring power from the gateway. Once power is restored, you may navigate to the IP address of the gateway as normal.



Security - Log Out

Once a user is done with a session they may click **logout** at the top of any page. The user may also be logged out for inactivity based off of the Log Out Timer specified during the configuration.



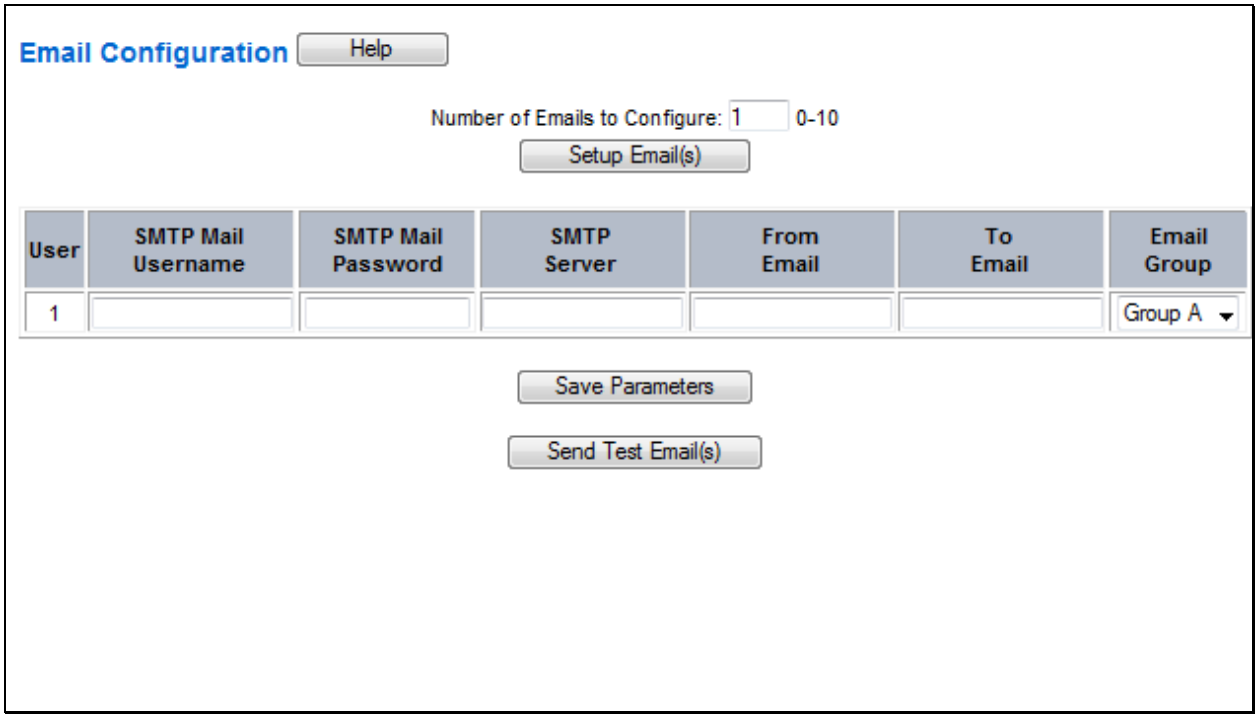
Closing the browser is not sufficient to log out.

Email Configuration

You can configure up to 10 email addresses.

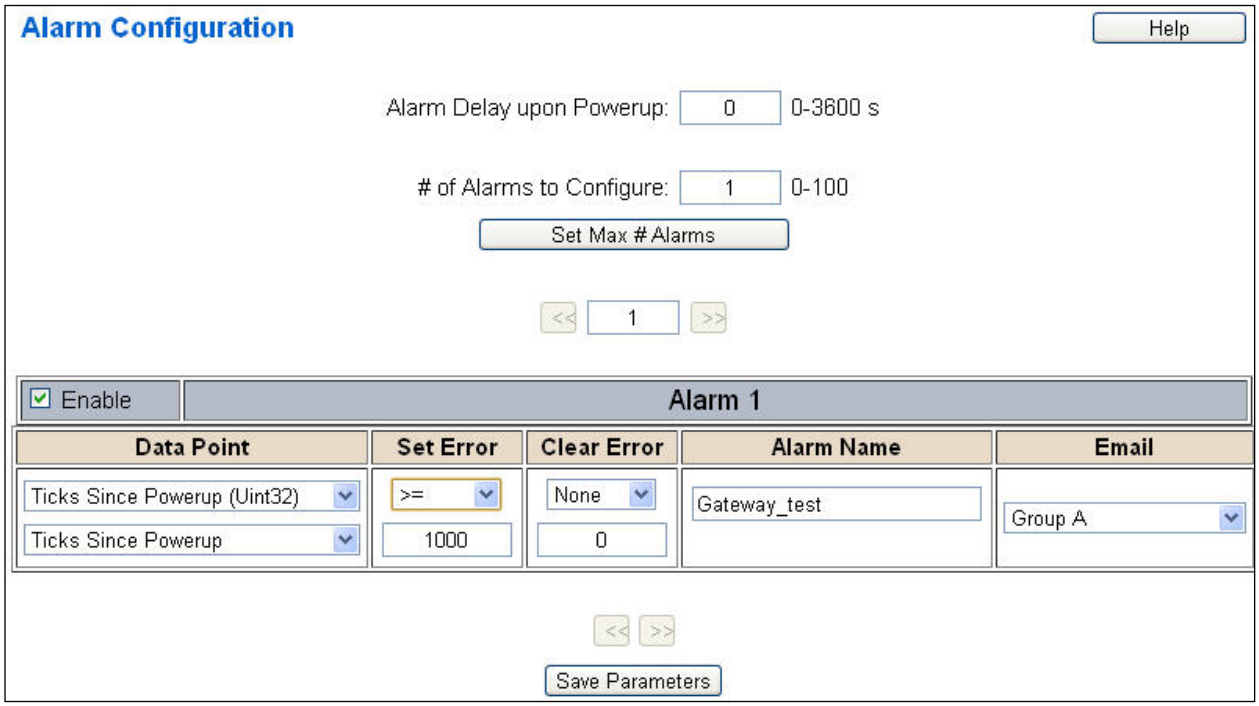
1. SMTP Mail Username: The email address that the smtp server has set up to use.
2. SMTP Mail Password: If authentication is required, enter the smtp Server's password (Optional).
3. SMTP Server: Enter the Name of the SMTP Server or the IP Address of the Server.
4. From E-mail: Enter the e-mail that will show up as the sender.
5. To E-mail: Enter the e-mail that is to receive the e-mail.
6. E-mail Group: Choose a group for the user. This is used in other web pages.

Click the **Save Parameters** button to commit the changes and reboot the gateway.



Alarm Configuration

1. Alarm Delay upon Powerup: At Powerup, the gateway will have values of '0' stored for all data. This may cause alarms to trigger before these values are updated by the mating protocols. Set this field to provide needed time to update fields before considering values for alarms.



2. Enter the number of alarms to configure and click **Set Max # Alarms** to generate those lines.
3. In the Data Point Section:
    a. Top dropdown: select the Data Group. This dropdown menu will contain all groups that go from the gateway to the network.
    b. Lower dropdown: select the Data Point's Specific Point. This is used to select which point in the group will be monitored for alarms.
4. In the Set Error Section:
    a. Select the Set Error Operation in the top dropdown menu. Available options are <, >, <=, >=, !=, ==, and Change of State (COS). This is the operation that will be used to compare the Data Point value against the Error Value to determine if the alarm needs to be set.
    b. Select the Set Error Value. This value is used as: 'Data Point's Value' 'Operation' 'Value.' Ex: Ticks Since Powerup >= 1000. This will set the alarm after 1000 ticks have elapsed since the unit powered up.

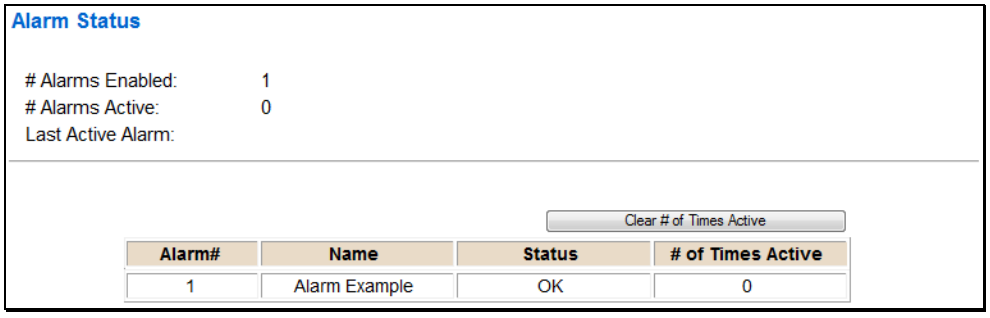
5. In the Clear Error Section:
    a. Select the Clear Error Operation. Available options are <, >, <=, >=, !=, ==, and Change of State (COS). This is the operation that will be used to compare the Data Point value against the Error Value to determine if the alarm needs to be cleared.
    b. Select the Clear Error Value.
    -Ex: Ticks Since Powerup >= 5000. This will clear the alarm after 5000 ticks have elapsed since the unit powered up.
6. Enter an Alarm Name. This will make the alarm unique and will be available in the Alarm Status page as well as in the email generated by the alarm.
7. Select an email to associate this alarm with. When an alarm is set, it sends an email. When an alarm is cleared, it will also send an email.

Click the **Save Parameters** button to commit the changes to memory and reboot the gateway.

Diagnostics – Alarm Status

Alarm Status will only display under the Diagnostic menu tab if at least 1 Alarm is enabled.

1. # Alarms Enabled: This is a count of enabled alarms.
2. # Alarms Active: This is how many alarms are presently active (set).
3. Last Active Alarm: This is the last alarm that the gateway detected.
4. **Clear # of Times Active**: This will reset all alarms '# of Times Active' to 0.
5. Alarm #: The reference number to the given alarm on the alarm setup page.
6. Name: The name of the alarm.
7. Status: The current status of the alarm, either OK or ALARM.
8. # of Times Active: This count represents the number of times this alarm has become active. If an alarm is triggered, this count will increment.

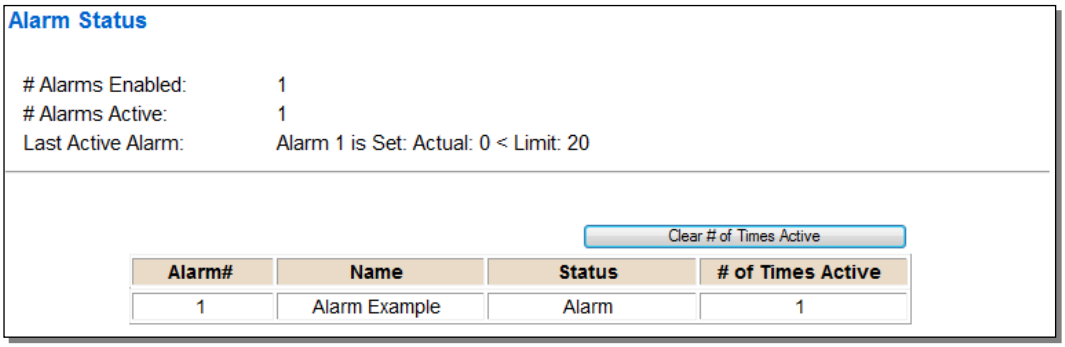

Alarm Status
Alarms Enabled: 1
Alarms Active: 0
Last Active Alarm:
Clear # of Times Active
Alarm# Name Status # of Times Active
1 Alarm Example OK 0

Alarms – Active

While one or more alarms are active, every page will display 'Alarms Active' at the top of the page. This will no longer be displayed if all active alarms have been cleared.

When an alarm is activated, the following will occur:

1. A one-time notification will be sent out to the email associated with the alarm.
    a. For duplicate emails to occur, the alarm must be cleared and then become active again.
2. *# Alarms Active* and *# of Times Active* will be incremented.
3. Status of the Individual Alarm will be set to *Alarm*.
4. *Last Active Alarm* field will be populated with details on what triggered the alarm.


Alarm Status
Alarms Enabled: 1
Alarms Active: 1
Last Active Alarm: Alarm 1 is Set: Actual: 0 < Limit: 20
Clear # of Times Active
Alarm# Name Status # of Times Active
1 Alarm Example Alarm 1

Alarms – Clear

When an alarm is cleared, the following will occur:

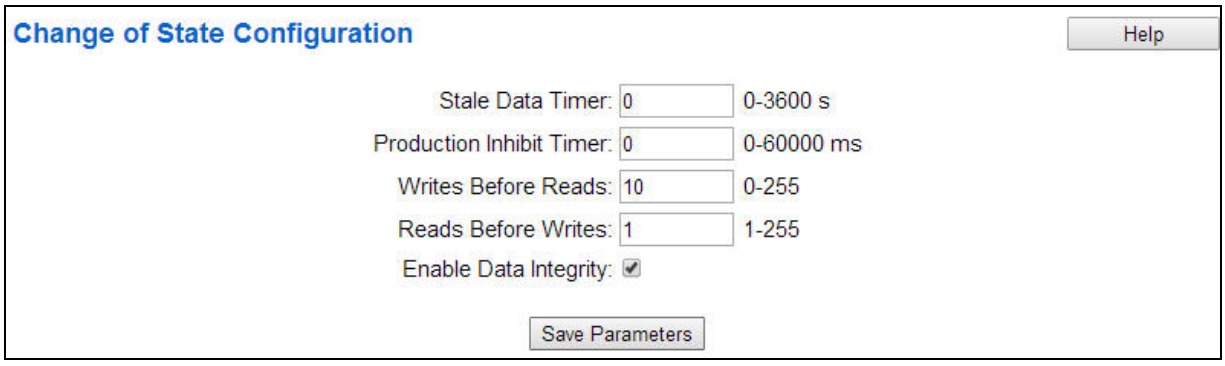
1. A one-time notification will be sent to the email associated with the alarm.
    a. For duplicate emails to occur, the alarm must become active and then be cleared again.
2. Total *# Alarms Active* will decrement. *Last Active Alarm* will not be changed.
3. Status of the Individual Alarm will be reset to *OK*.

Change of State (COS) Configuration

The gateway, by default only writes when data has changed. The gateway also waits to write any data to the destination until the source protocol is successfully connected.

Default values should fit most applications. Change these values with caution as they affect performance.

1. **Stale Data Timer**: If the data has not changed within the time allocated in this Stale Data Timer, the data will be marked as stale within the gateway and will force a write request to occur. This timer is to be used to force cyclic updates in the gateway, since data will only be written if it has changed by default. There is a separate timer per data mapping.
   Gateway behavior:
   If time = 0s => (DEFAULT) The gateway will write out new values on a Change of State basis.
   If time > 0s => The gateway will write out new values whenever the timer expires to force Cyclic updates (write every *x* seconds).
2. **Production Inhibit Timer:** Amount of time after a Change of State write request has occurred before allowing a new Change of State to be written. This is to be used to prevent jitter. Default value is 0ms. This timer takes priority over the Stale Data Timer. There is a separate timer per data mapping. This timer is active only after the first write goes out and the first COS event occurs.
3. **Writes Before Reads**: If multiple writes are queued, execute # of Writes Before Reads before the next read occurs. Default is 10 and should fit most applications. **Warning:** A value of 0 here may starve reads if a lot of writes are queued. This may be useful in applications where a burst of writes may occur and you want to guarantee they all go out before the next set of reads begin.
4. **Reads Before Writes:** If multiple writes are queued, the # of Writes Before Reads will occur before starting the # of Reads Before Writes. Once the # of Reads Before Writes has occurred, the counter for both reads and write will be reset. Default is 1 and should fit most applications.
5. **Enable Data Integrity**: If enabled, do not execute any write requests to the destination until the source data point is connected and communicating. This prevents writes of 0 upon power up.


Change of State Configuration
Help
Stale Data Timer: 0 0-3600 s
Production Inhibit Timer: 0 0-60000 ms
Writes Before Reads: 10 0-255
Reads Before Writes: 1 1-255
Enable Data Integrity:
Save Parameters

Click the **Save Parameters** button to commit the changes to memory and reboot the gateway.

Diagnostics Info

The Diagnostic page is where you will be able view the gateway's translations and protocol specific status information.

For protocol specific diagnostic information, refer to the next three pages.

Diagnostics – Data and String Mapping

The Diagnostics->Diagnostic Info->System section displays the number of translations that are enabled, for both Data and String data types, the number of mappings that have an error, and the first mapping that has an error.

 # Enabled: Number of mappings that are enabled.

 # Error: The number of mappings that are enabled that have an error.

First Error: This is a detailed description of the first mapping that has an error.

Common Errors:

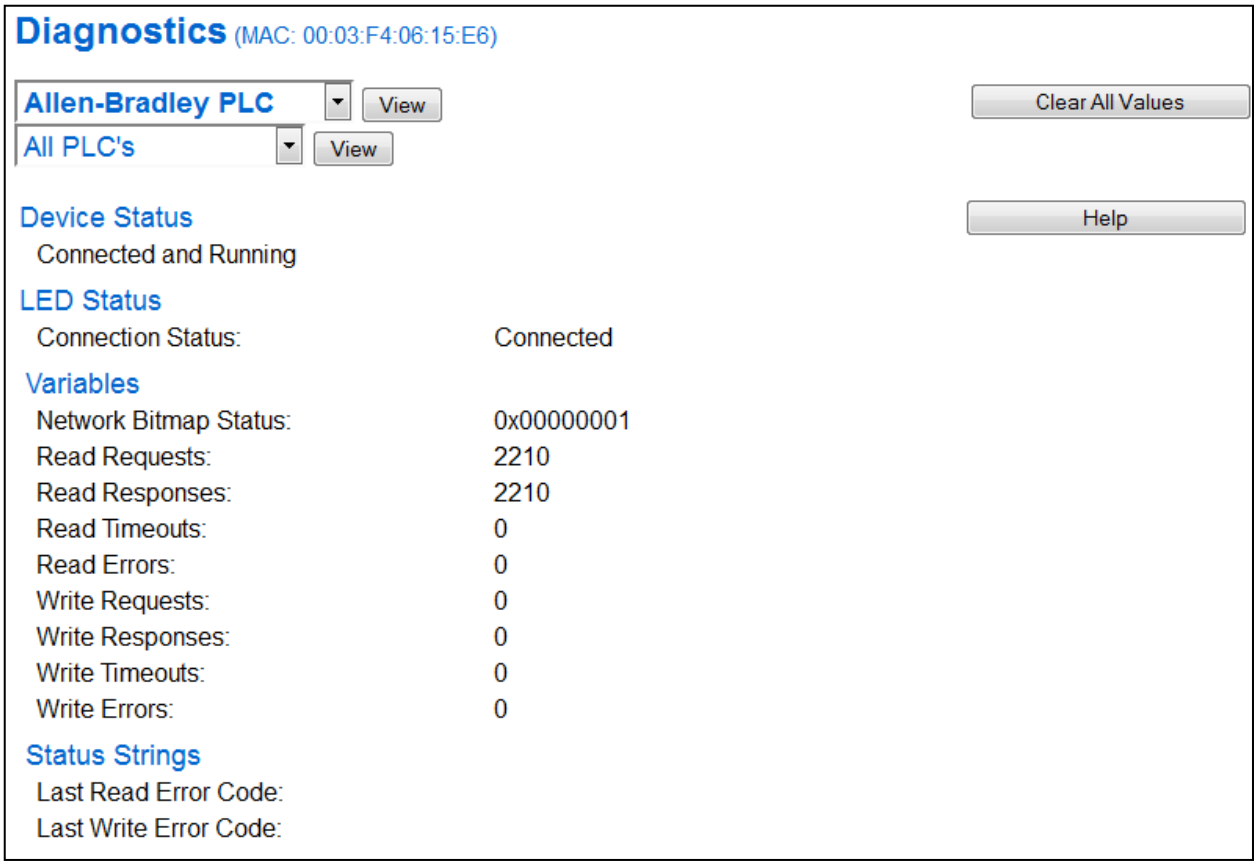
1. Destination or Source Point does not exist
   -Solution: Re-map the mapping
2. Source or Destination Pointer too small
   - There is not enough space on either the Source, or the Destination for the data you want to copy. This is typically seen when the Destination is smaller than the amount of data being transferred to it.
3. Range Discard, Min or Max Value
   - The actual data value is outside of the defined range
4. Math Error
   - Operation value cannot be 0
5. Scaling Error
   - Source Min must be smaller than Source Max
   - Destination Min must be smaller than Destination Max

Diagnostics – Allen-Bradley PLC

Select the **Allen-Bradley PLC** in the dropdown menu on the Diagnostic page to view a breakdown of the diagnostics and common strings that are displayed on the page. You may also view individual counters by selecting the device in the **All PLC's** dropdown menu and clicking **View**.

Device Status - This will only display when viewing *All PLC's*.

1. Connected – The gateway is connected to all of the PLC's that are configured and enabled.
2. Nodes Missing (timed out) – one or more enabled PLC's are missing.
3. Empty Scan List – No PLC's are configured.
4. Dependency Protocol Faulted – The dependent protocol is missing causing the communication to go to inactive.



LED Status - This is the Status for *All PLC's* or the specific PLC selected.

1. Connected (Solid Green) – All of the enabled PLC devices are connected and running.
2. Not Connected (Flashing Green) – No PLC's are enabled.
    a. Verify Allen-Bradley PLC settings and ensure that the *Enable* checkbox is checked for the appropriate device(s).
3. Connection Timeout (Flashing Red) – The gateway cannot open a connection to 1 or more of the enabled PLC's.
    a. Verify the IP, Slot and Controller type is accurate for the missing connection. Missing connection can be determined from the Network Bitmap Status value.
4. Communication not attempted yet (Flashing Red) – (Specific Server Only) No reads are configured and data needed for writes isn't valid yet.
5. Dependency Error (Flashing Red) – The dependent protocol is missing causing the communication to go to inactive.
    a. The other Protocol must be connected.

Variables - These are the values for *All PLC's* or the specific PLC selected.

1. Network Bitmap Status (hex) – each bit corresponds to a PLC. If the bit is set, then the PLC is connected, otherwise the bit is 0. Bit 0 (right most) is PLC 1 and Bit 4 is PLC 5.
2. Read Requests – Number of read requests sent from the gateway to the PLC (N2G).
3. Read Responses – Number of valid responses sent from PLC to the gateway (G2N).
4. Read / Write Timeouts – Since we are TCP based, the gateway will timeout on the read or write and close the TCP connection. This counter will not continually increment. The Bitmap will reflect the missing PLC.
5. Read Errors – Number of read error responses sent from the PLC to the gateway.
6. Write Requests – Number of write requests sent from the gateway to the PLC (G2N).
7. Write Responses – Number of valid write responses sent from the PLC to the gateway.
8. Write Errors – Number of write error responses sent from the PLC to the gateway.

Common Error Strings - These are the values for *All PLC's* or the specific PLC selected.

1. IP: xxx.xxx.xxx.xxx "tagname" (04) Path Segment Error – The tag name is wrong or the tag is not defined as a controller scope tag.
2. IP: xxx.xxx.xxx.xxx "tagname" (08) Service Not Supported – The IP Address or the Slot Number does not match with the PLC the gateway is setup to communicate with.
3. IP: xxx.xxx.xxx.xxx "tagname" (1E) Embedded Server Error – The tag name that is setup within the gateway doesn't match a tag setup in the PLC.
4. IP: xxx.xxx.xxx.xxx "tagname" (ff,2105) Access beyond end of array – Tried to read/write too much data.
5. IP: xxx.xxx.xxx.xxx "tagname" (ff, 2107) Abbreviated type mismatch – The data type of the tag, on a write, in the gateway doesn't match the tag in the PLC.

Diagnostics – Modbus RTU Slave

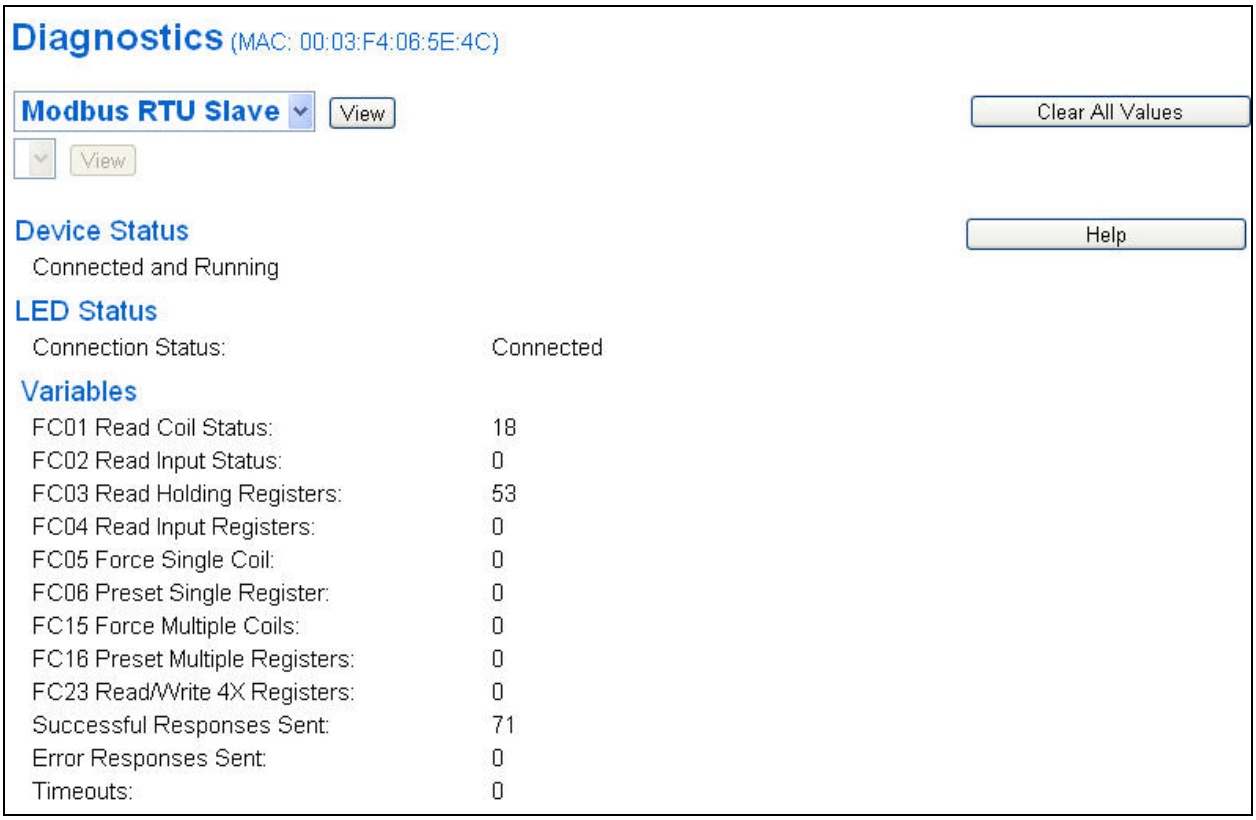
Select the **Modbus RTU Slave** in the dropdown menu on the Diagnostic page. Additional diagnostic information can be found by clicking on the **Help** button.

Clear All Values - *This will only affect Displayed Values.*

1. This will return all values displayed to 0 and clear the status string.
2. If Viewing Modbus RTU Slave, this will only clear the values for the Modbus RTU Slave section of the gateway.

Device Status

1. Connected - A Modbus RTU Master has a connection for the gateway.
2. Not Connected:
    a. The Modbus RTU Master has not opened up communication to the gateway.
    b. The Modbus RTU Master has not communicated to the gateway in "x" milliseconds, where "x" is the inactivity timeout specified in the Modbus RTU Slave Configuration.
3. Fatal Error: Hardware Port Not Configured:
    a. Hardware Port not configured in the Port Configuration web page.
    b. Hardware Port selected in the Modbus RTU Slave configuration page doesn't match the port configured.



Diagnostics – Modbus RTU Slave

LED Status:

1. Good Communication (Solid Green) – The gateway is connected to a Modbus RTU Master and communicating as expected.
2. Not Connected (Flashing Green) – The gateway has never been connected to a Modbus RTU Master.
3. Fatal Error (Solid Red) – The port configured does not match the port configured within the Modbus RTU configuration page.
4. Connection Timeout (Flashing Red) – The gateway has lost a connection to the Modbus RTU Master.

Variables:

1. FC01 Read Coil Status – Modbus Function Code 1: Number of Read Coil Status requests received.
2. FC02 Read Input Status – Modbus Function Code 2: Number of Read Input Status requests received.
3. FC03 Read Holding Registers – Modbus Function Code 3: Number of Read Holding Registers requests received.
4. FC04 Read Input Registers – Modbus Function Code 4: Number of Read Input Registers requests received.
5. FC05 Force Single Coil – Modbus Function Code 5: Number of Write Coil Status requests received.
6. FC06 Preset Single Register – Modbus Function Code 6: Number of Write Holding Register requests received.
7. FC15 Force Multiple Coils – Modbus Function Code 15: Number of Write multiple Coil Status requests received.
8. FC16 Preset Multiple Registers – Modbus Function Code 16: Number of Write multiple Holding Register requests received.
9. FC23 Read/Write 4X Register – Modbus Function Code 23: Number of Read/Write Holding Registers requests received.
10. Successful Responses Received – Total number of Read/Write messages sent by the gateway.
11. Error Responses Received = Total number of Read/Write errors sent by the gateway.
12. Timeouts – Total number of Inactivity Timeouts that have occurred.

LED Configuration

To modify the behavior of the LEDs on the 460 gateway, navigate to Other->Setup LEDs.

The LED Configuration page lets you configure the LEDs on the gateway.

Each LED may be set to Disabled, Protocol 1, or Protocol 2. If either Protocol is a Master/Client, you may set the LED to represent either all Slaves/Servers configured in our gateway or a particular Slave/Server device.

To select a particular Slave/Server device:

a) Select the protocol in the left dropdown menu.

b) Click **Save Parameters** to generate the second dropdown menu.

c) Select the individual Slave/Server in the right dropdown menu.

Click the **Save Parameters** button to commit the changes and reboot the gateway.

LED 1 is the LED closest to the Ethernet port on the gateway device.

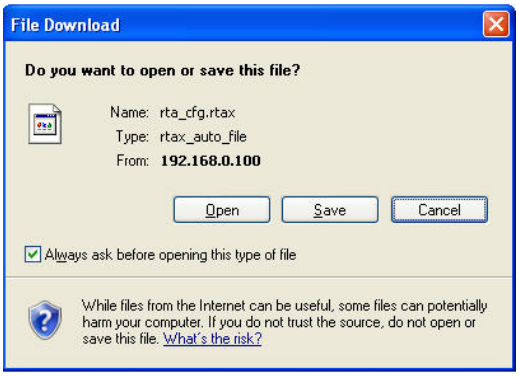
Configuration Files

To access the configuration files in the 460 gateway, navigate to other->Export/Import Config.

Export Configuration

The export tool allows you to save your gateway configuration for backup or to be exported into another gateway. This file is named *rta_cfg.rtax* by default. Network settings will not be saved in this configuration since they must be unique for each gateway.

Upon clicking the **Save Configuration to File** button, you will be prompted to select a location to save the file.


File Download
Do you want to open or save this file?
Name: rta_cfg.rtax
Type: rtax_auto_file
From: 192.168.0.100
Open
Save
Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Import Configuration

You can import a previously exported configuration file or a configuration file from another device into the 460 gateway whenever it is in Configuration Mode.

Upon clicking the **Choose File** button, you will be prompted to select a location from which to load the saved file. Once the location is selected, click the **Load Configuration** button.

If it has successfully loaded, the gateway will indicate that it was successful and a message will appear under the Load Configuration button indicating you should reboot the gateway.

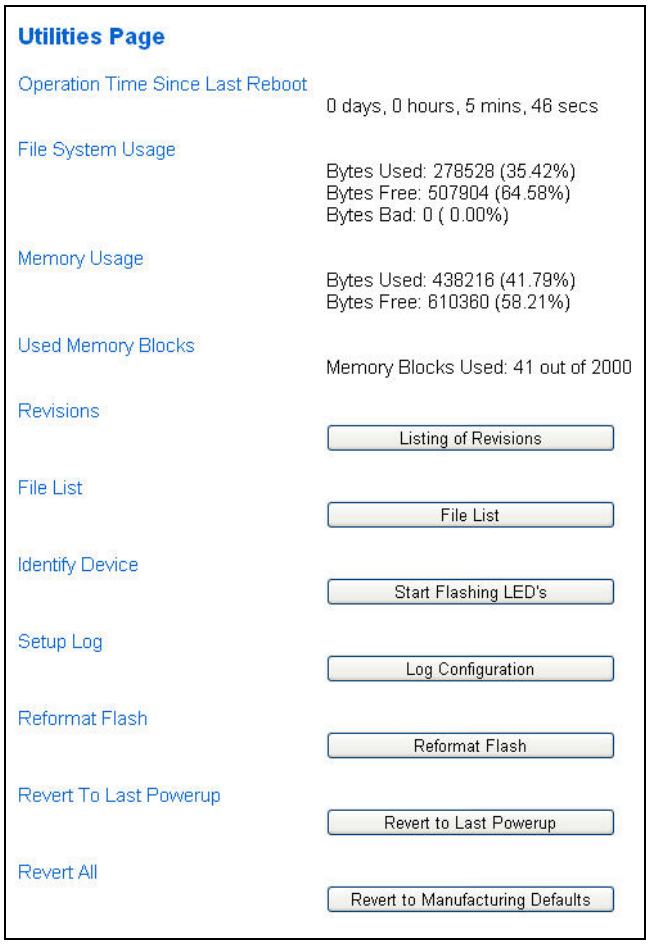
If it encountered an error while trying to load the saved configuration, the gateway will indicate the first error it found and a brief description about it under the Load Configuration button. The configuration file is xml and can be modified with any text editor. Once that error is fixed, try loading again until it is successful.

Utilities

The Utilities screen displays information about the gateway including Operation Time, File System Usage, Memory Usage, and Memory Block Usage.

Here you can also:

- View the Revisions of the Software for each Stack.
- View all of the Flash Files within the gateway.
- Identify your device by clicking the **Start Flashing LED's** button. By clicking this button, the two diagnostic LED's will flash red and green. Once you have identified which device you are working with, click the button again to put the LED's back into running mode.
- Configure the size of the Log through the Log Configuration.
- Remove the Configuration File and Flash Files within the gateway (the gateway needs to be rebooted 2 times).
- Bring the device back to its last power up settings.
- Bring the device back to its original manufacturing defaults (the Gateway needs to be rebooted 2 times).



Completing the Installation

You have now set up your gateway for communication and are ready to place the device in your application.

Support for your device is available any time.

Toll free: 800-249-1612
Email: support@rtaautomation.com